DIPLOMA IN INFORMATION TECHNOLOGY

NETWORKS 1 A

STUDY GUIDE
2023

TABLE OF CONTENTS

1. ABOUT BRAND

Damelin knows that you have dreams and ambitions. You're thinking about the future, and how the next chapter of your life is going to play out. Living the career you've always dreamed of takes some planning and a little bit of elbow grease, but the good news is that Damelin will be there with you every step of the way.

We've been helping young people to turn their dreams into reality for over 70 years, so rest assured, you have our support.

As South Africa's premier education institution, we're dedicated to giving you the education experience you need and have proven our commitment in this regard with a legacy of academic excellence that's produced over 500 000 world – class graduates! Damelin alumni are redefining industry in fields ranging from Media to Accounting and Business, from Community Service to Sound Engineering. We invite you to join this storied legacy and write your own chapter in Damelin's history of excellence in achievement.

A Higher Education and Training (HET) qualification provides you with the necessary step in the right direction towards excellence in education and professional development.

2. OUR TEACHING AND LEARNING METHODOLOGY

Damelin strives to promote a learning-centred and knowledge-based teaching and learning environment. Teaching and learning activities primarily take place within academic programmes and guide students to attain specific outcomes.

- A learning-centred approach is one in which not only lecturers and students, but all sections and activities of the institution work together in establishing a learning community that promotes a deepening of insight and a broadening of perspective with regard to learning and the application thereof.
- An outcomes-oriented approach implies that the following categories of outcomes are embodied in the academic programmes:
- Culminating outcomes that are generic with specific reference to the critical cross-field outcomes including problem identification and problem-solving, co-operation, selforganisation and self-management, research skills, communication skills, entrepreneurship and the application of science and technology.
- Empowering outcomes that are specific, i.e. the context specific competencies students must master within specific learning areas and at specific levels before they exit or move to a next level.
- Discrete outcomes of community service learning to cultivate discipline-appropriate competencies.

Damelin actively strives to promote a research culture within which a critical-analytical approach and competencies can be developed in students at undergraduate level. Damelin accepts that students' learning is influenced by a number of factors, including their previous educational experience, their cultural background, their perceptions of particular learning tasks and assessments, as well as discipline contexts.

Students learn better when they are actively engaged in their learning rather than when they are passive recipients of transmitted information and/or knowledge. A learning-oriented culture that acknowledges individual student learning styles and diversity and focuses on active learning and student engagement, with the objective of achieving deep learning outcomes and preparing students for lifelong learning, is seen as the ideal. These principles are supported through the use of an engaged learning approach that involves interactive, reflective, cooperative, experiential, creative or constructive learning, as well as conceptual learning via online-based tools.

Effective teaching-learning approaches are supported by:

- Well-designed and active learning tasks or opportunities to encourage a deep rather than a surface approach to learning.
- Content integration that entails the construction, contextualization and application of knowledge, principles and theories rather than the memorisation and reproduction of information.
- Learning that involves students building knowledge by constructing meaning for themselves.

- The ability to apply what has been learnt in one context to another context or problem.
- Knowledge acquisition at a higher level that requires self-insight, self-regulation and selfevaluation during the learning process.
- Collaborative learning in which students work together to reach a shared goal and contribute to one another’s learning at a distance.
- Community service learning that leads to collaborative and mutual acquisition of competencies in order to ensure cross cultural interaction and societal development.
- Provision of resources such as information technology and digital library facilities of a high quality to support an engaged teaching-learning approach.
- A commitment to give effect teaching-learning in innovative ways and the fostering of digital literacy.
- Establishing a culture of learning as an overarching and cohesive factor within institutional diversity.
- Teaching and learning that reflect the reality of diversity.
- Taking multi culturality into account in a responsible manner that seeks to foster an appreciation of diversity, build mutual respect and promote cross-cultural learning experiences that encourage students to display insight into and appreciation of differences.

2.1. Icons

The icons below act as markers, that will help you make your way through the study guide.

📎	**Additional information** Find the recommended information listed.
⬇	**Case study/Caselet** Apply what you have learnt to the case study presented.
🔍	**Example** Examples of how to perform a calculation or activity with the solution / appropriate response.
📌	**Practice** Practice the skills you have learned.

📚	**Reading** Read the section(s) of the prescribed text listed.
👓	**Revision questions** Complete the compulsory revision questions at the end of each unit.
☑	**Self-check activity** Check your progress by completing the self-check activity.
👥	**Study group / Online forum discussion** Discuss the topic in your study group or online forum.
💡	**Think point** Reflect, analyse and discuss, journal or blog about the idea(s).
▶	**Video / audio** Access and watch/listen to the video/audio clip listed.
☰	**Vocabulary** Learn and apply these terms.

3. INTRODUCTION TO THE MODULE

Welcome to NETWORKS 1A

3.1. Module Information

Qualification title	DIPLOMA IN INFORMATION TECHNOLOGY
Module Title	NETWORKS 1A
NQF Level	6
Credits	360

Notional hours	150

3.2. Module Purpose

The objective of this module is to introduce and develop the student's understanding of networks and its components. It is also aimed at developing students' skills in understanding the importance of networking and the various types that exist.

3.3. Outcomes

At the end of this module learners should be able to know:

- LAN and WAN communications are explained and applied.
- Network communication protocols are described and used correctly.
- Different types of network cable media are explored and a cabled network is designed.
- Devices for connecting networks are explained and a router-based network is designed.
- Current wireless networking technologies are explored and design options for wireless networks are considered.
- Sharing resources on a network is explained and a peer-to-peer office network is designed.
- A server is installed and set up, and a server-based office network is designed.
- WAN connection choices are explored and a network for WAN connectivity is designed.
- Factors that affect network design are investigated and a network for an office or organization is designed.
- Several network security issues are explored and security into home and office networks is designed.
- Hardware and software methods to monitor a network is explained and a solutions strategy for network troubleshooting is designed.

3.4. Assessment

You will be required to complete both formative and summative assessment activities.

Mark allocation

The marks are derived as follows for this module:

Test	20
Assignment	20

Exam	60
TOTAL	100%

3.5. Pacer

The table below will give you an indication of which topics you need to include from the module pacer.

Week	Topics
1	THE BUSINESS OF NETWORKING
2	UNDERSTANDING NETWORKING
3	UNDERSTANDING NETWORK CABLING
4	UNDERSTANDING NETWORK HARDWARE
5	MAKING WAN CONNECTIONS
6	UNDERSTANDING NETWORK PROTOCAOLS
7	EXPLORING DIRECTORY SERVICES
8	NETWORK REMOTE ACCESS
9	NETWORK SECURITY
10	NETWORK DISASTER RECOVERY
11	NETWORK SERVERS
12	PURCHASING AND MANAGING CLIENT COMPUTERS
13	DESIGNING A NETWORK

3.6. Planning Your Studies

You will have registered for one or more modules in the qualification and it is important that you plan your time. To do this look at the modules and credits and units in each module.

Create a time table / diagram that will allow you to get through the course content, complete the activities, and prepare for your tests, assignments and exams. Use the information provided above (How long will it take me?) to do this.

What equipment will I need?

- Access to a personal computer and internet.

This module will take you approximately **xxxxx hours** to complete. The following table will give you an indication of how long each module will take you.

Unit Number	Hours
1	1
2	1
3	1
4	1
5	1
6	1
7	1

8	1
9	1
10	1
11	1

4. PRESCRIBED READING

4.1. Prescribed Book

- The CompTIA Network+ Certification Kit by Todd Lammle.
- CompTIA Network+ Certification All-in-One Exam Guide, Sixth Edition by Mike Meyers.

4.2. Recommended Articles

- https://docs.microsoft.com/
- https://www.stormshield.com/
- https://www.sciencedirect.com/
- https://structuredcabling.com/
-

4.3. Recommended Multimedia

Websites:

- https://docs.microsoft.com/
- https://www.networkworld.com/
- https://www.networkcomputing.com/

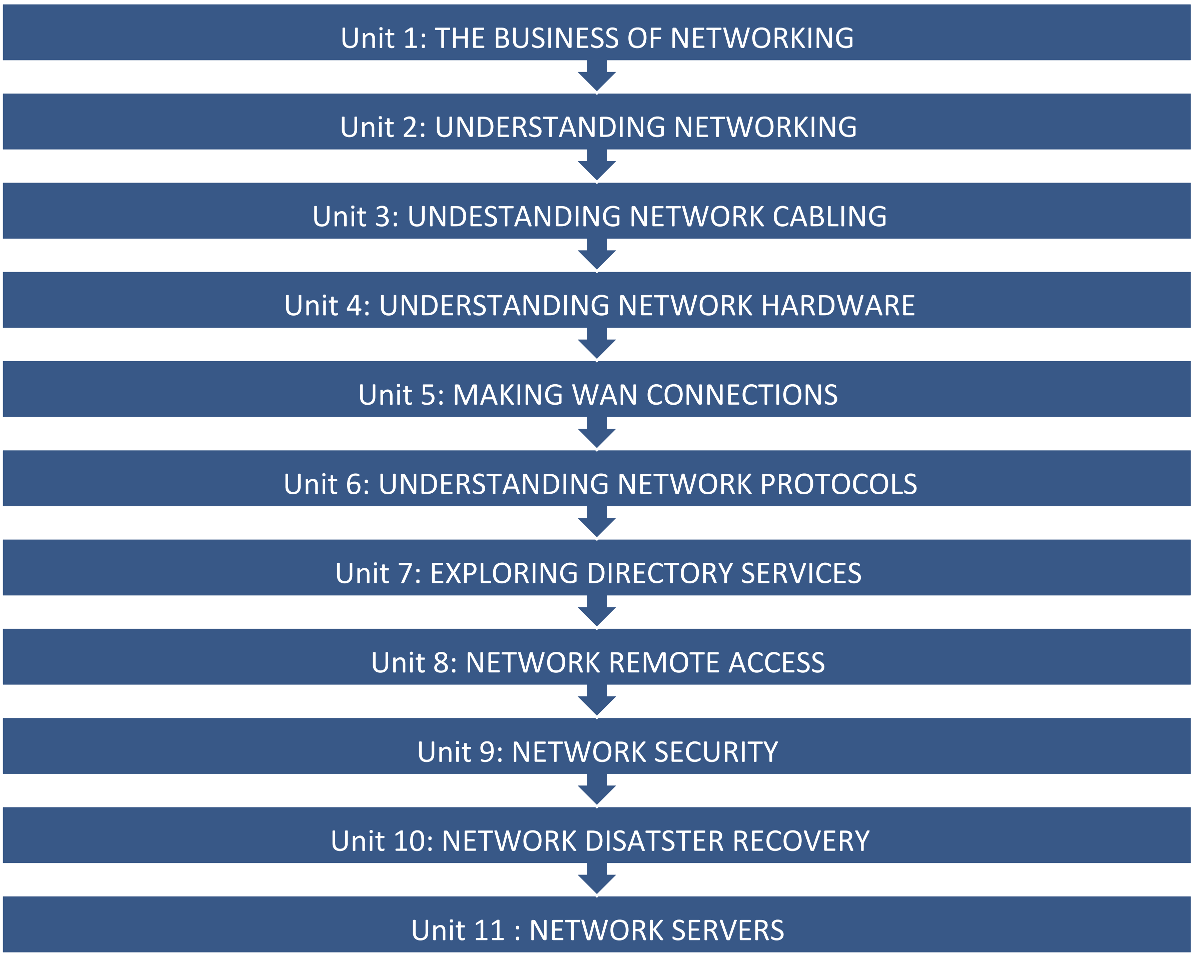
Video / Audio

-

5. MODULE CONTENT

You are now ready to start your module! The following diagram indicates the topics that will be covered. These topics will guide you in achieving the outcomes and the purpose of this module.

Please make sure you complete the assessments as they are specifically designed to build you in your learning.



Unit 1: THE BUSINESS OF NETWORKING

Unit 2: UNDERSTANDING NETWORKING

Unit 3: UNDESTANDING NETWORK CABLING

Unit 4: UNDERSTANDING NETWORK HARDWARE

Unit 5: MAKING WAN CONNECTIONS

Unit 6: UNDERSTANDING NETWORK PROTOCOLS

Unit 7: EXPLORING DIRECTORY SERVICES

Unit 8: NETWORK REMOTE ACCESS

Unit 9: NETWORK SECURITY

Unit 10: NETWORK DISATSTER RECOVERY

Unit 11 : NETWORK SERVERS

5.1. THE BUSINESS OF NETWORKING

Purpose	The purpose of this unit is to ensure the learner knows how networking has impacted technology today, what companies are benefiting from implementing networks and the roles played by network administrators.
Learning Outcomes	By the end of this unit, you will be able to: • Understanding Networking: The Corporate Perspective • What Does the Company Need? • Understanding Networking: The Corporate Perspective • What Does the Company Need? • Understanding Networking: The Corporate Perspective
Time	It will take you 45 minutes to make your way through this unit.

Important terms and definitions	• Network Administrator • MCSE

6. INTRODUCTION

This book is a soup-to-nuts beginner's guide to networking. Before delving into the bits and bytes of networking, which are covered in the rest of the book, you should start by understanding the whys and wherefores of networking. This study unit discusses networking from a business perspective. You'll learn about the benefits that networking brings a company and the different types of networking jobs available. You'll also discover how networks are supported from the business perspective, and how you can begin a career in networking. Finally, you'll learn about the SarbanesOxley Act of 2002 and how its requirements affect networking professionals.

Understanding Networking: The Corporate Perspective

To be truly effective in the field of networking, you need to start by understanding networking from the corporate perspective. Why are networks important to companies? What do they accomplish for the company? How can networking professionals more clearly meet the needs of the company with the networks that they build and maintain? It's important to realize that there are no single correct answers to these questions. Every company will have different needs and expectations with regard to their network. What is important is that you learn the relevant questions to ask about networking for your company and arrive at the best possible answers to those questions for your particular company. Doing so will ensure that the company's network best meets its needs.

What Does the Company Need?

There are many possible reasons that a company might need or benefit from a network. In order to understand your particular company, you should start by exploring the following questions. You may need to ask a variety of different people in the company their perspective on these questions. Some of the managers that you may need to interview include the chief executive officer or owner, the chief financial officer, and the heads of the various key departments within the company, such as manufacturing, sales and marketing, accounting, purchasing and materials, retail operations, and so forth. The range of managers that you interview will depend on the type of business in which the company is engaged. It's important that you first start by understanding the business itself and the business-oriented perspectives of these different individuals and the people in their departments. Consider the following questions for each of these key areas of the organization:

- What is their function for the company?
- How do their objectives tie into the company objectives?
- How might information technology (IT) play a role in supporting their objectives?

- What sorts of automation do they think might help them accomplish their objectives?
- How is the work in their area accomplished? For instance, do most of the employees do mechanical work, like on a production line, or are most of them so-called “knowledge workers” who generate documents, analyze information, and so forth?
- What are the key inputs for the functional area, in terms of information or materials, and what are the key outputs for the functional area? What processes convert the inputs into the outputs?

Your objective in asking these questions, and others that may occur to you, is to get a good understanding of each functional area: what it does and how it does it, as well as what it wants to be able to do in the future. With this knowledge, you can then start to analyze the impact that the network—or improvements to the existing network— might have in those various areas. Beginning from a business perspective is absolutely essential. Networks are not built and improved “just because.” Instead, any particular network or network upgrade needs to be driven by the needs of the business. Justifications for networks or improvements to existing networks should clearly show how they are necessary to the proper functioning of the business, or how they will play an important role in the company achieving its objectives, consistent with the cost and effort involved.

How Will the Network Benefit the Company?

17 After getting a good understanding of the company, its objectives, and how it accomplishes its work, you can then analyze different ideas that you may have for the network, and how those ideas will benefit some or all parts of the business. In doing so, you need to consider at least the following areas:

- Are there any areas in which the lack of a network, or some failing of the existing network, is inhibiting the company from realizing its goals or accomplishing its work? For example, if an existing network is undersized and this causes people to waste too much time on routine tasks (such as saving or sending files, or compiling programs), what improvements might address those shortcomings? Or maybe the network and its servers are unreliable, and so people are frequently losing their work or are unproductive while problems are addressed.

- Are there capabilities that you could add to the network that would provide benefits to the business? For example, if many people in the company are constantly sending faxes (for instance, salespeople sending price quotations to customers), would adding a network-based fax system produce significant productivity benefits? What about other network-based applications? (Study unit3 lists some common network features that you may want to review to help in answering this question.)

- What other automation plans exist that will require the support of the network? For example, say you’re the network administrator in a company. What new applications or features will be added to the network that you need to support? Is the company planning on installing some kind of videoconferencing system, for instance? If so, do you know what changes you will need to make to the network to support the system?

- What needs to be done to the network simply to maintain it? In most companies, file space requirements grow rapidly, even if the business itself isn’t expanding. How much additional storage space does the network need to keep going forward? How many additional servers and other components will be needed to keep the network working smoothly?

Obviously, a list such as the preceding one can’t be exhaustive. The important point is that you need to approach the job of networking first from the perspective of the company and its needs. Within that framework, use your creativity, knowledge, experience, and business and technical acumen to propose and execute a plan for the network. The remainder of this book discusses the information you need to start learning about this important part of any company's infrastructure.

Understanding Networking Jobs

If you're planning on entering the field of networking (and this book is designed as a good start for that), it's important to have some understanding of the various networking jobs that you're likely to encounter and what they typically require. Of course, actual job requirements will vary widely 18 between companies and for different established networks. Also, companies may have different entry-level opportunities through which you can enter a networking career. The following descriptions are broad overviews of some key jobs.

Network Administrator

A network administrator is responsible for keeping an organization's computer network up-to-date and operating as intended. Any company or organization that uses multiple computers or software platforms needs a network admin to coordinate and connect the different systems. Seems simple enough—but there's another common IT job title that is commonly confused: systems administrator.

Network administrator vs. systems administrator

You may be wondering if a network administrator is essentially the same as a systems administrator. In short—not really. But the lines can blur depending on the work environment. In many smaller organizations, the terms "network administrator" and "systems administrator" are often interchangeable as they may cover the same tasks.

That being said, the differences between network and systems administrators become much clearer in large organizations. The best way to differentiate between the two is to examine the type of work they do—so let's dive in.

Top technical skills for network administrators

We used real-time job analysis software to examine nearly 150,000 network administrator jobs posted over the past year.[2] This helped us determine the top technical skills employers are seeking:

- System administration
- Linux®
- Microsoft Active Directory®
- VMware®
- Technical support
- Windows Server®
- Cisco®
- Hardware and software installation
- SQL
- Customer service https://www.rasmussen.edu/degrees/technology/blog/what-does-a-network-administrator-do/

STUDY UNIT SUMMARY

Many people I've met who work in some area of information technology, such as networking, don't consider the business reasons for the network when they go about their day-to-day jobs or when they propose improvements to the network. This certainly isn't limited to the field of networking; many people who work in any area of a company sometimes forget that the reason their function exists is to support the objectives of the company in which they work. The most successful employees of any company keep firmly in mind why they do what they do, before they consider how best to do it. Some of the suggestions in this study unit should help you to approach managing and improving a network successfully, by keeping in mind the benefits the network brings to the company. Once you know what the company needs, then you can then propose the best solutions to solve problems that arise or make appropriate improvements to the network.

5.1.2 Revision Questions

Answer the compulsory revision questions below.

1. Name three duties of a Network Administrator
2. How can information technology play a role in your organization?
3. Are there any areas in which the lack of a network, or some failing of the existing network, is inhibiting the company from realizing its goals or accomplishing its work?
4. What are the key inputs for the functional area in terms of information or materials, and what are the key outputs for the functional area?

https://www.youtube.com/watch?v=4BM3zPTTj4g

https://www.youtube.com/watch?v=cNwEVYkx2Kk

https://www.youtube.com/watch?v=7OwjgxkuypI

7. UNDERSTANDING NETWORKING

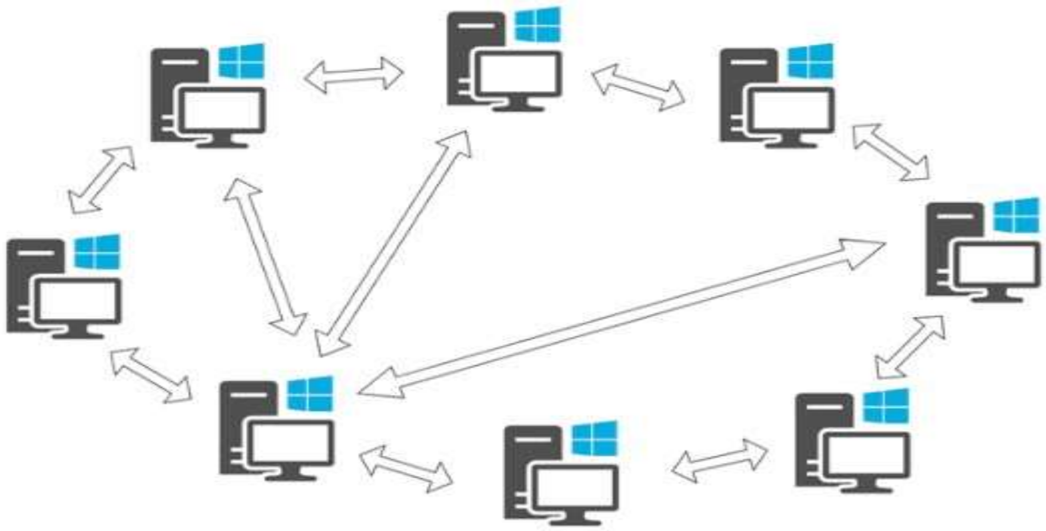
Purpose	The purpose of this unit is to ensure the learner knows different types of networks, the pro's and cons of those networks and the OSI Reference model.
Learning Outcomes	By the end of this unit, you will be able to: • Understanding How Data Travels Through the OSI Layers • Understanding the OSI Networking Model • Learning Network Features • Client/Server Network Relationships • Peer-to-Peer Network Relationships • Knowing Network Relationship Types
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• OSI • RAS • LAN • WAN

5.2.1: INTRODUCTION

There are a lot of aspects to networking, and this tends to make the subject seem] more complex than it really is. This study unit discusses some basic and key networking concepts. If you're new to networking, getting a good understanding of the subjects in this study unit will enable you to build a mental framework into which you can fit more detailed knowledge as it is presented in the remainder of this book. In addition, the rest of this book assumes you're comfortable with all the concepts presented in this study unit.

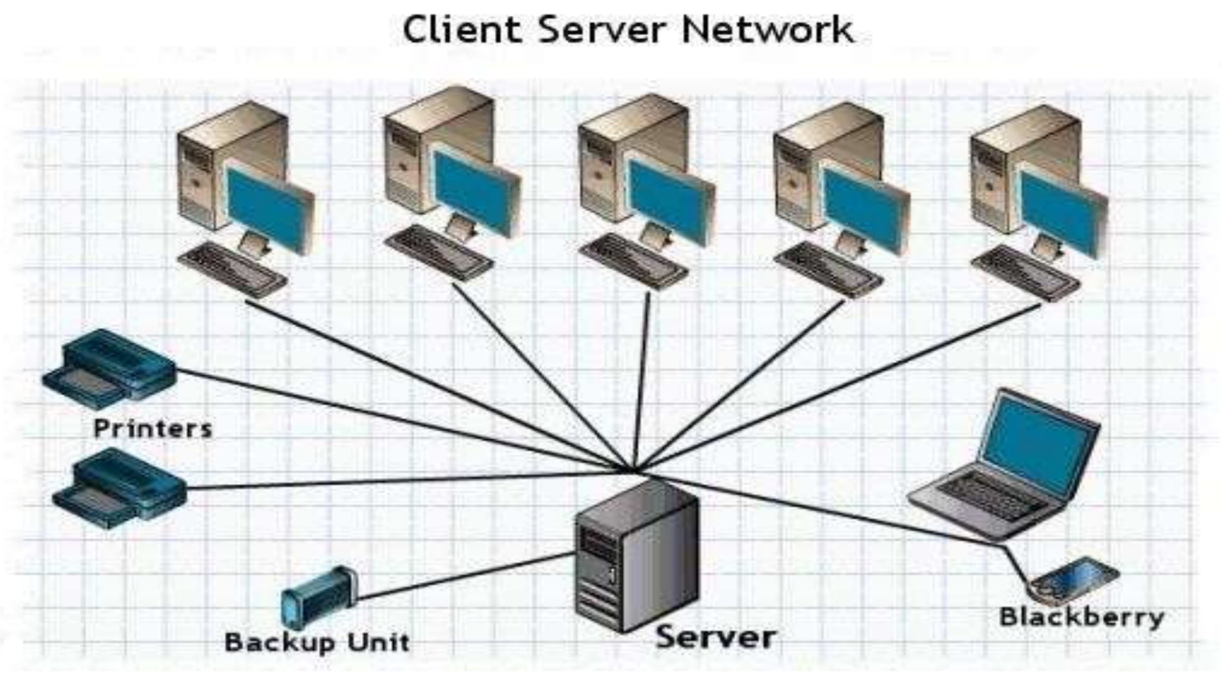
Peer-to-Peer Network

In a peer-to-peer network relationship, the computers on the network communicate with each other as equals. Each computer is responsible for making its own resources available to other computers on the network. These resources might be files, directories, application programs, devices (such as printers, modems, or fax cards), or any combination of these items. Each computer is also responsible for setting up and maintaining its own security for those resources. Additionally, each computer is responsible for accessing the network resources it needs from other peer-to-peer computers, knowing where those resources are located in the network, and handling the security required to access them.

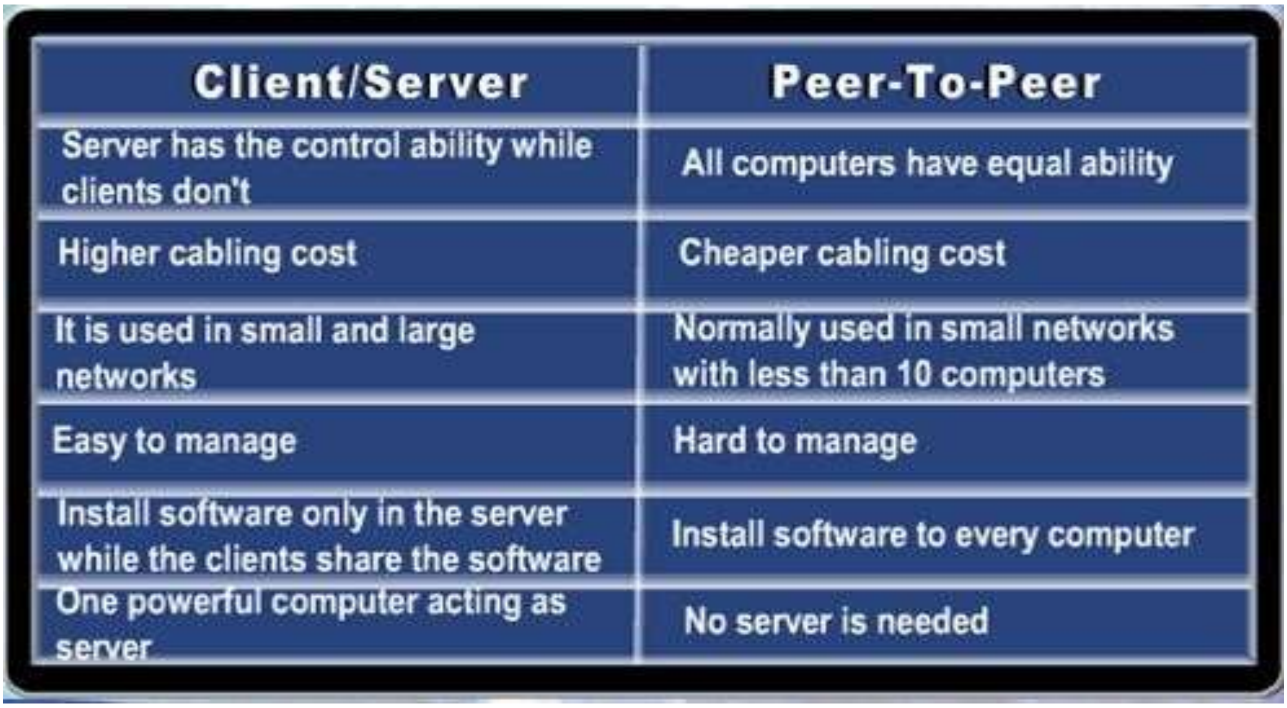


Client/Server Network Relationships

In a client/server network relationship, a distinction exists between the computers that make available network resources (the servers) and the computers that use the resources (the clients, or workstations). A pure client/server network is one in which all available network resources—such as files, directories, applications, and shared devices—are centrally managed and hosted, and then are accessed by the client computers. None of the client computers share their resources with other client computers or with the servers. Instead, the client computers are pure consumers of these shared network resources.



CLIENT SERVER VS PEER TO PEER NETWORKS



Client/Server	Peer-To-Peer
Server has the control ability while clients don't	All computers have equal ability
Higher cabling cost	Cheaper cabling cost
It is used in small and large networks	Normally used in small networks with less than 10 computers
Easy to manage	Hard to manage
Install software only in the server while the clients share the software	Install software to every computer
One powerful computer acting as server	No server is needed

NETWORK TYPES

There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

Local Area Network (LAN)

1. Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc.

2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

Metropolitan Area Network (MAN)

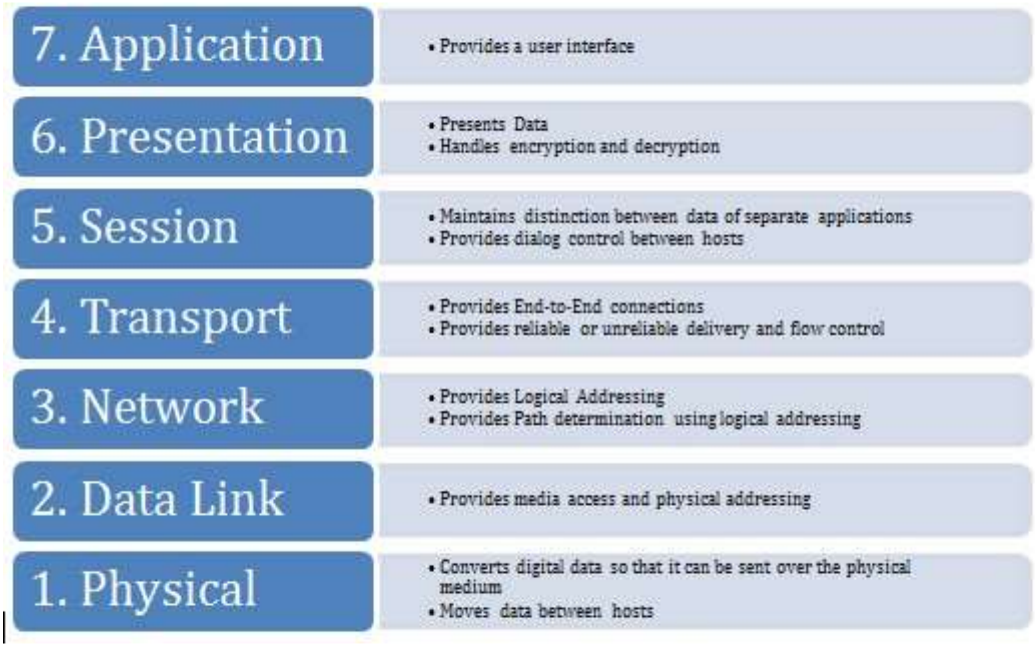
MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town

Wide area network (WAN)

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an

example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc

THE OSI MODEL



7. Application	• Provides a user interface
6. Presentation	• Presents Data • Handles encryption and decryption
5. Session	• Maintains distinction between data of separate applications • Provides dialog control between hosts
4. Transport	• Provides End-to-End connections • Provides reliable or unreliable delivery and flow control
3. Network	• Provides Logical Addressing • Provides Path determination using logical addressing
2. Data Link	• Provides media access and physical addressing
1. Physical	• Converts digital data so that it can be sent over the physical medium • Moves data between hosts

STUDY UNIT SUMMARY

This study unit introduced a number of important networking concepts. You learned about how computers on a network relate to one another, how the different parts of a network connection are logically broken down in the OSI network model, and how this model is useful in understanding networks. You also learned about a number of basic network features and resources. The following study units cover these subjects in more detail, starting with the next study unit, which discusses the often-misunderstood world of network wiring.

5.1.3 Revision Questions

Answer the compulsory revision questions below.

1. Name 5 protocols that operate at the Application layer of the OSI model
2. Which type of connectors are found on the Physical Layer of the OSI model
3. Explain the terms LAN,WAN and MAN.
4. Name 2 encryption programs that work at the Presentation Layer
5. Name 2 physical devices that work at Layer 2 of the OSI model

https://www.youtube.com/watch?v=4_zSIXb7tLQ

https://www.youtube.com/watch?v=-0thZyLPoBM

https://www.youtube.com/watch?v=vv4y_uOneC0

8. UNDERSTANDING NETWORK CABLING

Purpose	The purpose of this unit is for the learner to know how networks are layed out through the use of topologies, understand the various types of cables used in networking today.
Learning Outcomes	By the end of this unit, you will be able to: • Understanding Cable Topologies • Comparing Rings to Stars and Buses • Overview of Basic Cable Types • Installing and Maintaining Network Cabling
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• TOPOLOGIES • UTP/STP • SMF/MMF • CAT • MAU

5.3.1 INTRODUCTION

If you were to compare a computer network to the human body, the network cabling system would be the nerves that make up the physical manifestation of the nervous system. The network cabling system is what actually carries all the data from one point to another and determines how the network works. How a network is cabled is of supreme importance to how the network functions, how fast it functions, how reliable the network will be as a whole, and how easy it will be to expand and change the network. With any new network, your first task after assessing the needs for the network is to determine how the network should be wired; all the other components of the network are then built on that foundation. This is much like the OSI seven-layer model you learned about in Study unit 2, in that the network cabling makes up layer 1 (the physical layer), and all the upper networking layers rely on it.

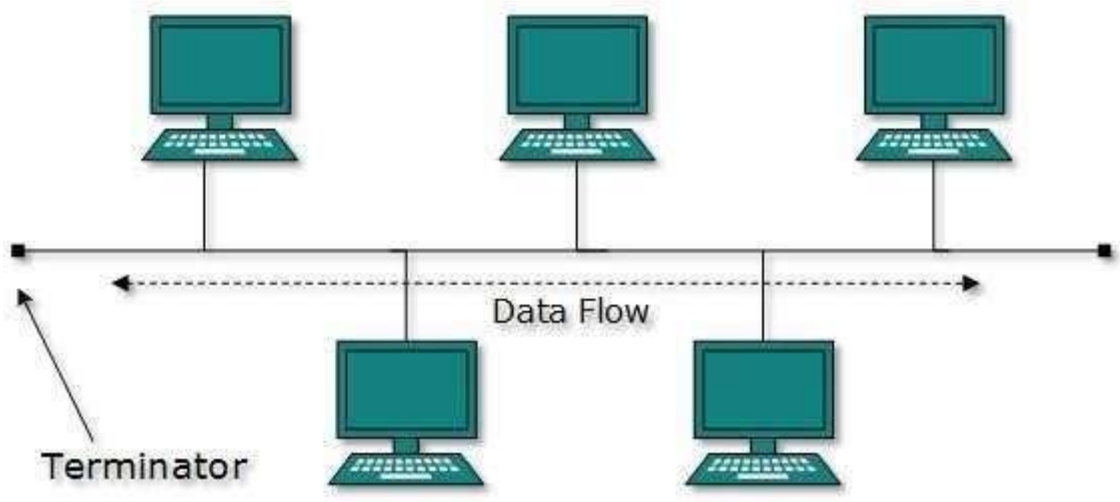
Many people think that network cabling is relatively simple. After all, what could be simpler than running a wire between two points? However, as you will see, the topic of network cabling encompasses more than meets the eye, and it’s an extremely important area to get right. If you make mistakes selecting or installing network cable, your network will likely be unreliable and may perform poorly. Because of the labor costs involved in wiring a network, the best time to address any potential problems in this area is well before they occur

TOPOLOGIES

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Bus Topology

In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

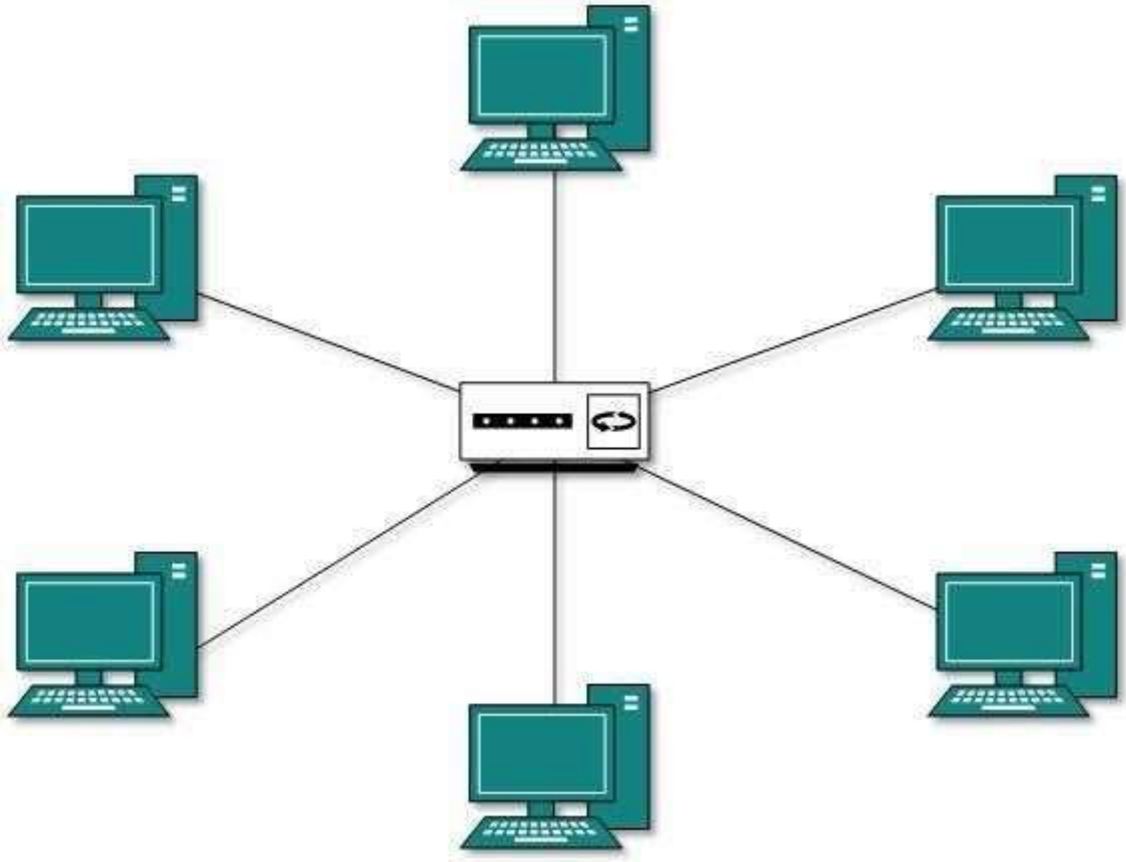


Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-topoint connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

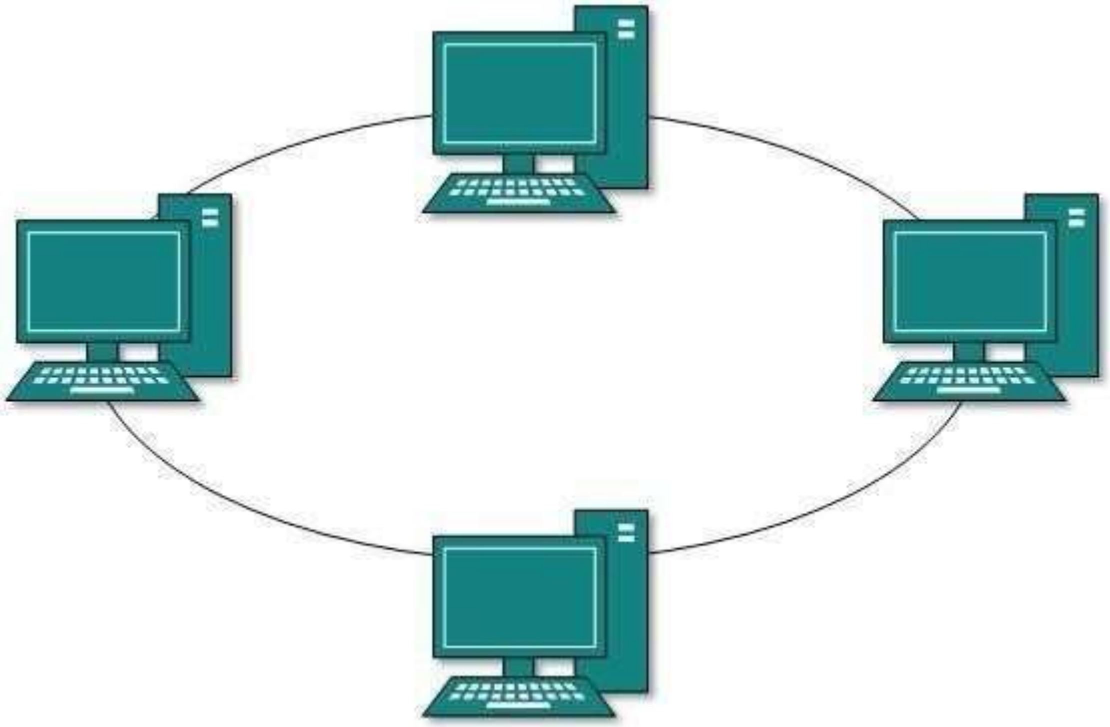
- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub.Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring Topology

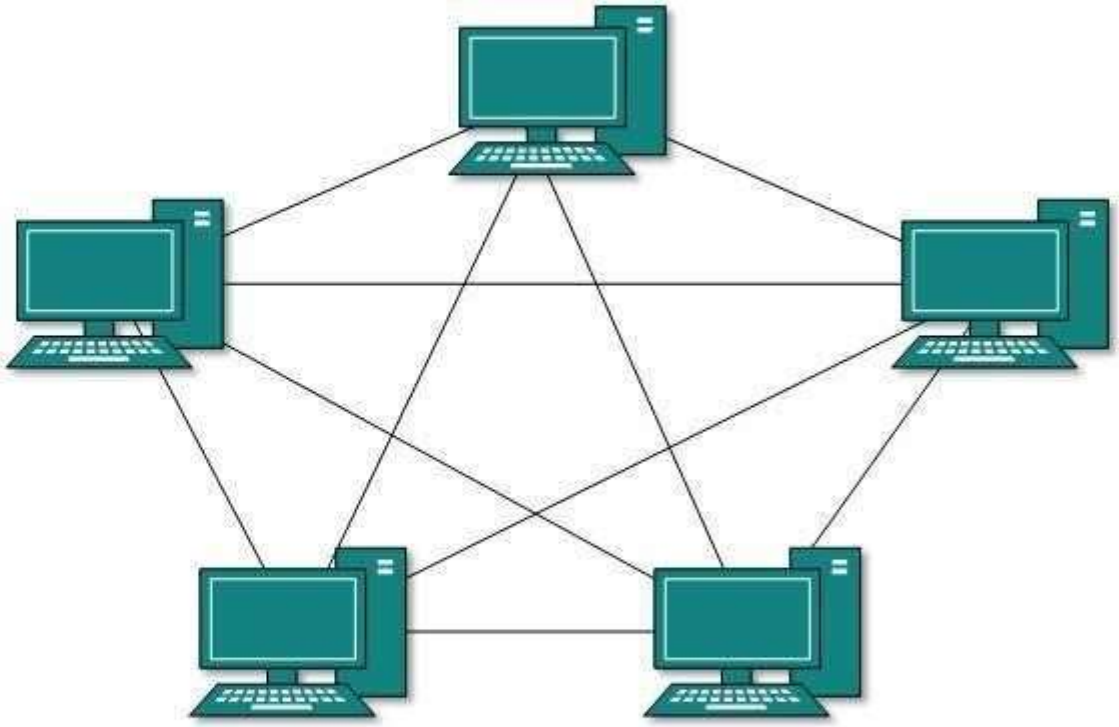
In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring.Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts.This topology has hosts in pointto-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

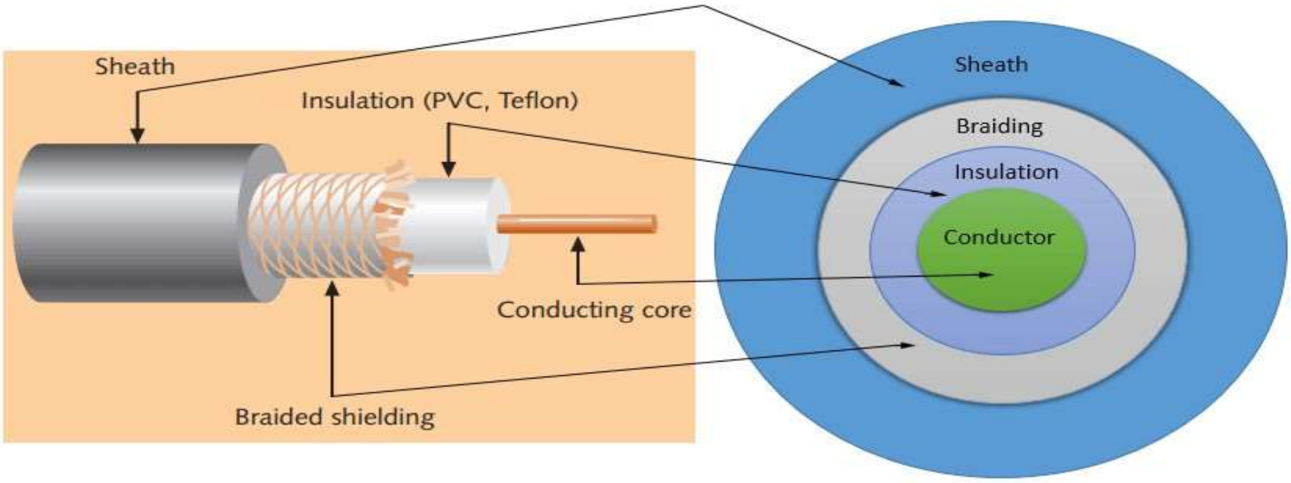
  https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm#:~:text=Advertisements,different%20in%20a%20same%20network.

Overview of Basic Cable Types

Coaxial cable

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.

The following image shows these components.



Twisted-pair cables

The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable.

This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

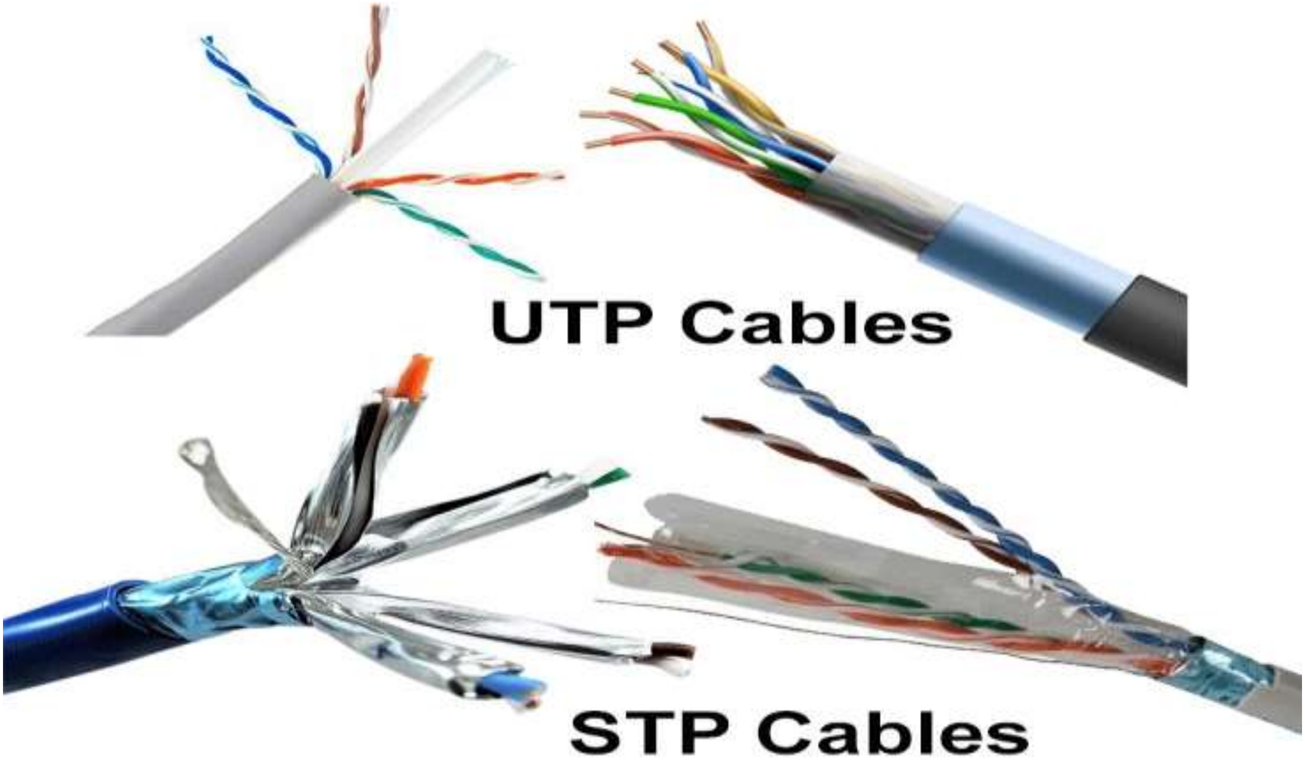
In the **UTP (*Unshielded twisted-pair*) cable**, all pairs are wrapped in a single plastic sheath.

In the **STP (*Shielded twisted-pair*) cable**, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

6. Similarities and differences between STP and UTP cables

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Since the STP cable contains more materials, it is more expensive than the UTP cable.
- Both cables use the same RJ-45 (registered jack) modular connectors.
- The STP provides more noise and EMI resistant than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.
- Both cables can accommodate a maximum of 1024 nodes in each segment.

The following image shows both types of twisted-pair cable.



The TIA/EIA specifies standards for the twisted-pair cable. First standards were released in 1991, known as **TIA/EIA 568**. Since then, these standards have been continually revised to cover the latest technologies and developments of the transmission media.

The TIA/EIA 568 divides the twisted-pair cable into several categories. The following table lists the most common and popular categories of the twisted-pair cable.

Category / name of the cable	Maximum supported speed	Bandwidth/support signals rate	Ethernet standard	Description
Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4 pairs). This cable was used in the token-ring network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.
Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twistedpairs and shields each pair by its own plastic sheath.

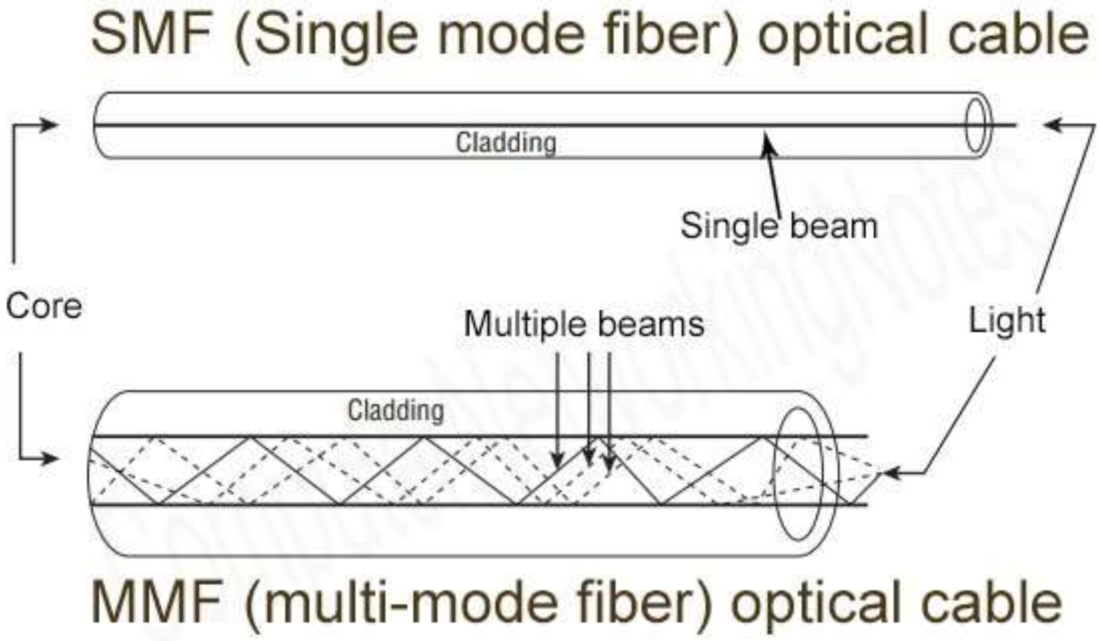
Fiber optic cable

This cable consists of core, cladding, buffer, and jacket. The core is made from the thin strands of glass or plastic that can carry data over the long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

- Core carries the data signals in the form of the light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.


SMF (Single mode fiber) optical cable
Cladding
Single beam
Core
Multiple beams
Light
Cladding
MMF (multi-mode fiber) optical cable

SMF (Single-mode fiber) optical cable

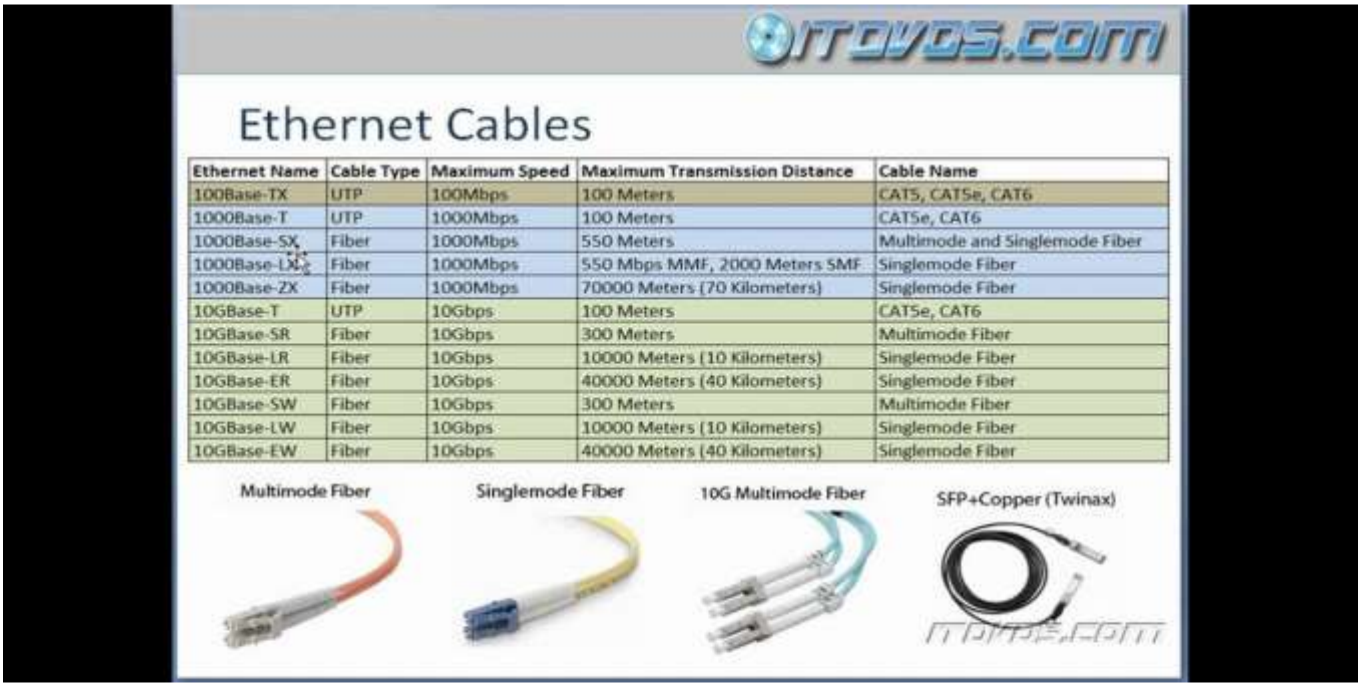
This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable

This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used in shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.

That's all for this tutorial. In the next part of this article, we will understand the types of connectors that are used to connect cables with networking devices. If you like this tutorial, please don't forget to share it with friends through your favorite social channel.

https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-andspecifications.html



Ethernet Cables

Ethernet Name	Cable Type	Maximum Speed	Maximum Transmission Distance	Cable Name
100Base-TX	UTP	100Mbps	100 Meters	CAT5, CAT5e, CAT6
1000Base-T	UTP	1000Mbps	100 Meters	CAT5e, CAT6
1000Base-SX	Fiber	1000Mbps	550 Meters	Multimode and Singlemode Fiber
1000Base-LX	Fiber	1000Mbps	550 Mbps MMF, 2000 Meters SMF	Singlemode Fiber
1000Base-ZX	Fiber	1000Mbps	70000 Meters (70 Kilometers)	Singlemode Fiber
10GBase-T	UTP	10Gbps	100 Meters	CAT5e, CAT6
10GBase-SR	Fiber	10Gbps	300 Meters	Multimode Fiber
10GBase-LR	Fiber	10Gbps	10000 Meters (10 Kilometers)	Singlemode Fiber
10GBase-ER	Fiber	10Gbps	40000 Meters (40 Kilometers)	Singlemode Fiber
10GBase-SW	Fiber	10Gbps	300 Meters	Multimode Fiber
10GBase-LW	Fiber	10Gbps	10000 Meters (10 Kilometers)	Singlemode Fiber
10GBase-EW	Fiber	10Gbps	40000 Meters (40 Kilometers)	Singlemode Fiber

STUDY UNIT SUMMARY

In this study unit, you learned about network cable systems. It covered the major topologies in which networks are wired, how CSMA/CD and token passing work, what types of cables are commonly used, and how they should be installed. You also learned some tips about selecting cabling contractors and troubleshooting network cable problems. The next study unit expands on this discussion by focusing on creating small office or home office networks. As part of that discussion, you will also learn about wireless networking.

5.1.4 Revision Questions

Answer the compulsory revision questions below.

a) Which physical topology is the most fault tolerant?
b) Which topology uses termination at the end?
c) What is the difference between physical topology and logical topology?
d) Explain SMF as compared to MMF?
e) What is a CAT5?

https://www.youtube.com/watch?v=_NX99ad2FUA

https://www.youtube.com/watch?v=lAOE2aciNmw

https://www.youtube.com/watch?v=ktTtAQIvYkg

https://www.youtube.com/watch?v=lullzS740wI

9. UNDERSTANDING NETWORK HARDWARE

Purpose	The purpose of this unit is for the learner to be able to identify and know the functionalities of the different type of hardware used in networking.
Learning Outcomes	By the end of this unit, you will be able to: • Networking Components • Internet connection devices
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• Switches • Routers • REPEATERS • WIFI

5.4.1 INTRODUCTION

If network wiring constitutes the nervous system of a network, then the devices discussed in this study unit represent the various organs. These network devices— repeaters, routers, hubs, and such—are responsible for moving data from one network cable to another. Each device has different properties and uses. A good network design uses the correct device for each of the various jobs the network must fulfill. In this study unit, you learn about essential networking hardware, including the following:

- Repeaters
- Hubs and concentrators
- Switches
- Bridges
- Routers

Repeaters

A repeater is a device that extends the distance of a particular network run. It takes a weak network signal in on one side, boosts the signal, and then sends it out its other side. You most often see repeaters on Thin Ethernet networks, but they are available for virtually any network connection. For instance, if you need to run a 100Base-T Cat-5 cable longer than 100 meters (328 feet), a repeater enables you to double that distance. Repeaters operate at the physical layer of the OSI networking model. They do not have the intelligence to understand the signals they are transmitting. Repeaters merely amplify the signal coming in either side and repeat it through their other side. (Remember that they also amplify any noise on the cable!) Repeaters are used to connect only the same type of media, such as 10Base-2 Thin Ethernet to 10Base-2 Thin Ethernet, or Token Ring twisted-pair to Token Ring twisted-pair. In practice, repeaters are usually used with 10Base-2 networks (Thin Ethernet), which are discussed in Study unit 3. Repeaters do have a small amount of intelligence that can be useful. They can separate one of their connections from the other when there is a problem. For example, consider two segments of Thin Ethernet that are connected using a repeater. If one of those segments is broken, the repeater allows the good segment to continue working within itself. Users on the good segment will be unable to connect to resources on the broken segment, but they can still use the good segment without trouble. (But remember that this capability does you little good if your servers are on the broken segment and your workstations are on the good segment!)

Hubs and Concentrators

Intelligent LAN concentrators—usually just called concentrators or, even more simply, hubs—are used to connect network nodes to network backbones. Nodes are connected to hubs in a physical star fashion (cables fan out from the hub to each node); whether they are used for a star topology or a ring topology network (these topologies are discussed in Study unit4). A simple network might consist of just a hub or two; smaller networks usually don't require a network backbone. Hubs are available for virtually any network media type, with the higher-end units using replaceable study units to support multiple media types. For example, you can purchase a high-end hub chassis that can house both Ethernet and Token Ring study units. You can purchase hubs in a variety of sizes, ranging from those that support only 2 workstations to those that support more than 100 workstations. Many network designers use stackable hubs, which usually support 24 node connections each. These hubs are often used in concert with switches, which are discussed in the next section. Hubs have two important properties:

- Hubs echo all data from each port to all the other ports on the hub. Although hubs are wired in a star fashion, they actually perform electrically (logically) more like a bus topology segment in this respect. Because of this echoing, no filtering or logic occurs to prevent collisions between packets being transmitted by any of the connected nodes.
- Hubs can automatically partition (in this context, cut off) a problematic node from the other nodes—in effect, shutting down that node. Such partitioning occurs if a cable short is detected, if the hub port is receiving excessive packets that are flooding the network, or if some other serious problem is detected for a given port on the hub. Automatic partitioning keeps one malfunctioning connection from causing problems for all of the other connections. Hubs are becoming much more sophisticated. They often have a number of advanced built-in features, including the following:
- Built-in management, where the hub can be centrally managed over the network, using SNMP or other network management protocols and software.
- Autosensing of different connection speeds. For example, Ethernet hubs that can automatically detect and run each node at either 10 Mbps (10Base-T) or 100 Mbps (100BaseT) are common. 55
- High-speed uplinks that connect the hub to a backbone. These usually operate at ten times the basic speed of the hub. (For example, for a 100 Mbps hub, the uplink ports might run at 1 Gbps.)
- Built-in bridging and routing functions, which make it unnecessary to use separate devices to perform bridging and routing.
- Built-in switching, where nodes on the hub can be switched instead of shared.

Switches

Switches are a key component of many business networks, as they connect multiple PCs, printers, access points, phones, lights, servers, and other hardware. Switches allow you to send and receive information (such as email) and access shared resources in a smooth, efficient, highly secure, and transparent manner.

What is an unmanaged switch?

An unmanaged network switch is designed so that you can simply plug them in and they work, no configuration required. Unmanaged switches are typically for basic connectivity. You'll often see them used in home networks or wherever a few more ports are needed, such as at your desk, in a lab, or in a conference room.

What is a managed switch?

Managed switches give you greater security and more features and flexibility because you can configure them to custom-fit your network. With this greater control, you can better protect your network and improve the quality of service for those who access the network.

Routers

How does a router work?

Routers guide and direct network data, using packets that contain various kinds of data—such as files, communications, and simple transmissions like web interactions.
The data packets have several layers, or sections, one of which carries identifying information such as sender, data type, size, and most importantly, the destination IP (Internet protocol) address. The router reads this layer, prioritizes the data, and chooses the best route to use for each transmission.

Types of routers

Core router

Core routers are generally used by service providers (i.e. AT&T, Verizon, Vodafone) or cloud providers (i.e. Google, Amazon, Microsoft). They provide maximum bandwidth to connect additional routers or switches. Most small businesses will not need core routers. But very large enterprises that have many employees working in various buildings or locations may use core routers as part of their network architecture.

Edge router

An edge router, also called a gateway router or just "gateway" for short, is a network's outermost point of connection with external networks, including the Internet.

Edge routers are optimized for bandwidth and designed to connect to other routers to distribute data to end users. Edge routers don't usually offer Wi-Fi or the ability to manage local networks fully. They typically have only Ethernet ports—an input to connect to the Internet and several outputs to connect additional routers.

Edge router and modem are somewhat interchangeable terms, though the latter term is no longer commonly used by manufacturers or IT professionals when referencing edge routers.

Distribution router

A distribution router, or interior router, receives data from the edge router (or gateway) via a wired connection and sends it on to end users, typically via Wi-Fi, though the router usually also includes physical (Ethernet) connections for connecting users or additional routers.

Wireless router

Wireless routers, or residential gateways, combine the functions of edge routers and distribution routers. These are commonplace routers for home networks and Internet access.
Most service providers provide full-featured wireless routers as standard equipment. But even if you have the option to use an ISP's wireless router in your small business, you may want to use a business-level router to take advantage of better wireless performance, more connectivity controls, and security.

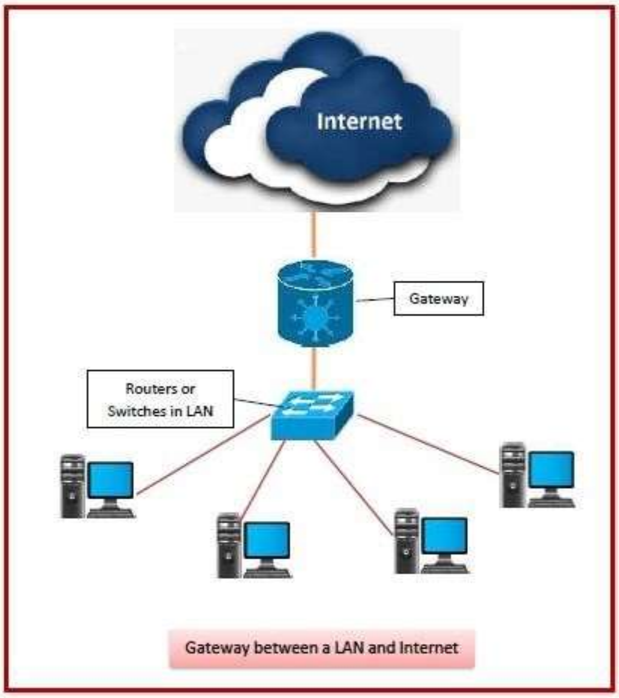
Virtual router

Virtual routers are pieces of software that allow some router functions to be virtualized in the cloud and delivered as a service. These routers are ideal for large businesses with complex network needs. They offer flexibility, easy scalability, and a lower entry cost. Another benefit of virtual routers is reduced management of local network hardware

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-arouter.html#~types-of-routers

Gateways

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.


Internet
Gateway
Routers or Switches in LAN
Gateway between a LAN and Internet

Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

Types of Gateways

On basis of direction of data flow, gateways are broadly divided into two categories −

- **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

STUDY UNIT SUMMARY

In this study unit, you learned about the key pieces of hardware that make up most networks. It is important for you to be familiar with the capabilities of all these types of network hardware, which should form the basis of any network design or performance-tuning efforts. Be aware that you need to know about other types of network hardware as well. Additional important network hardware is discussed in later study units. In particular, you should also know about remote access hardware, hardware that supports WAN links, and certain network functions that are carried out on different types of network servers. Study unit 5 discusses the different technologies used to connect networks to other networks, usually over large distances. WAN connections are used to connect to the internet and also to form part-time or full-time connections between LANs, such as from one company location to another

5.1.5 Revision Questions

Answer the compulsory revision questions below.

A. What is the difference between a repeater and an amplifier?
B. Why would it be better to use a switch rather than a hub?
C. Bridges work at which layer of the OSI model?

D. Routers work at which layer of the OSI model?

https://www.youtube.com/watch?v=YqRHaR-OQVQ https://www.youtube.com/watch?v=CVrYEPHexB4

https://www.youtube.com/watch?v=1z0ULvg_pW8

10. MAKING WAN CONNECTIONS

Purpose	The purpose of this unit is for the learner to be able to have in depth knowledge on wide area network technologies used in enterprise networks.
Learning Outcomes	By the end of this unit, you will be able to: • WAN Connection types
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• POTS • ISDN • DSL • ADSL • ATM

5.4.2 INTRODUCTION

Many companies have multiple locations that need to share network resources. For example, maybe the company's accounting system runs at the headquarters building where the accounting and MIS staff are located, but the warehouse across town still needs access to the accounting system for inventory picking tickets, data entry, and other order fulfillment and inventory tasks. Or, perhaps the company uses a groupware system such as Lotus Notes that requires regular updates of information and messages from one site to another. In the real world, the situation can become even more complex. Some companies have offices all around the globe, and each office has different requirements both to access and update data in other locations.

All of these are situations in which a wide area network (WAN) can be useful. Certainly, in a pinch, multiple offices can exchange data by using Federal Express and identical tape machines, CD-R discs, external USB hard disks, or other media. Sure, it's possible to simply send the data back and forth like this (assuming the application supports exchanging data in this fashion), but such an arrangement has some drawbacks—the biggest one being that it is pretty slow. There are many ways to connect local area networks (LANs) in one location to LANs in another location, and making such connections is the subject of this study unit

Determining WAN Needs

Think of a WAN as a connected system of local area networks, also known as LANs. These are the familiar one-campus company setups in which all offices are wired together. Keep in mind there are also MANs, or metropolitan area networks — connected sets of buildings across a city or town. MANs can figure into the WAN system as well.

In this example, your organization has a number of LANs. Imagine they're in Boston, New York, and Chicago. To span the distances between these three cities, your company either engages a leased line between each location — a leased line being a dedicated connection set up by your service provider — or the organization plugs into the public telecommunications network. Security, in these cases, is most often ensured through a virtual private network.

At each endpoint of the connections to the Boston, Chicago, and New York LANs, your business operates a router that allows the LAN to communicate with a hub that's handling incoming and outgoing data on the WAN side. Packets of information start to flow back and forth. Your WAN solution is in place.

Why Does a WAN Matter to the Enterprise?

WAN matters to business communications because it empowers enterprises to solve for high-speed connectivity while, in most cases, maintaining costs at scale.

If not for WANs, your organization would face the prospect of having to own and install every single mile of hardware when attempting to connect its three LANs in the example above. Instead, WANs take a far less costly approach, leveraging public systems to link one part of the organization to another across large distances.

Beyond the issue of cost, WANs also open a number of new options to businesses looking to make the most of their employees' time, no matter where they might be located. The ability to work remotely while also having secure access to company network assets are among the examples of how WANs benefit enterprises.

All this, however, is just the start of the story. WANs, it turns out, are evolving even further.

https://www.vonage.com/resources/articles/what-is-wan/

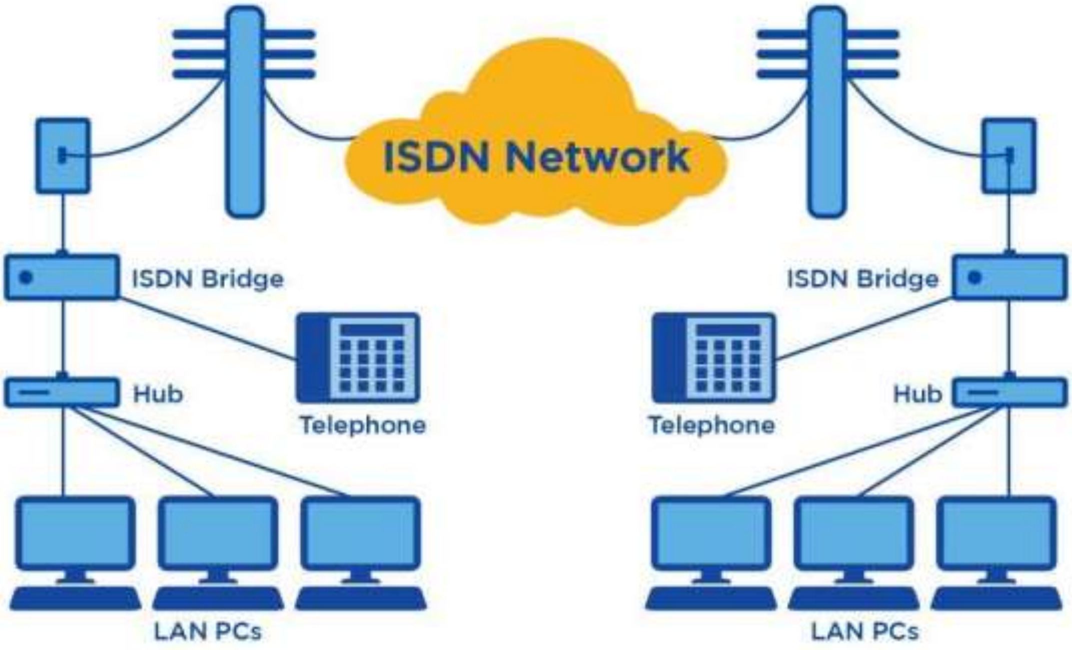
WAN Connection Types

Plain Old Telephone Service (POTS)

Plain old telephone service (POTS) is the telephone service everyone knows. While it does not technically qualify as a WAN connection (at least as most people think of WANs), POTS can still serve to link two or more sites together for certain low bandwidth needs. Although it is among the slowest methods of establishing a network connection, POTS is ubiquitous and easily used throughout the world. POTS are carried over one set of twisted-pair wires (in other words, just two wires). In some cases, two sets of twisted-pair wires are used, but only the two main wires carry the telephone signal and ring signals. The other two wires are used for other features, such as backlighting a keypad on a phone or providing a message-waiting light with some PBX systems. POTS connections currently use RJ-11 telephone jacks, which simply snap into place. The maximum theoretical speed of basic analog POTS is 33.6 Kbps. Many factors can decrease this speed; chief among them is line quality. Telephone lines with static typically do not connect at the top speed of 33.6 Kbps, and they might lose their connections unexpectedly, lose data being transmitted, or pause for excessive periods of time as bursts of static inhibit the ability to transfer data. When you are using POTS to establish a network connection, having matched modems at both ends is optimal. Matched modems from the same manufacturer more easily negotiate the highest possible data transmission rates and often can support “step-down” modes, which automatically use a slower speed when line noise unexpectedly becomes a problem. POTS transmits analog signals, not digital ones. The data sent between systems is converted from digital data to analog data using a modem. The word modem is actually an acronym based on the device’s function—modulator/demodulator. At each end of the connection, the sending system’s modem modulates the digital data into an analog signal and sends the signal over the telephone line as a series of audible sounds. At the receiving end, the modem demodulates the audible analog signal back into digital data for use with the computer. With much higher speed Internet connections being ubiquitous these days, POTS is not often used for transmitting data, except in extremely rare cases. However, given its heavy past use, and the remote chance that you might run into a system using a POTS connection for some type of data transmission, you should be familiar with it.

Integrated Services Digital Network (ISDN)

ISDN stands for Integrated Services Digital Network. It is a high-speed digital communications network based on existing telephone services. Although it has existed for more than ten years, because of extensive upgrades required at telephone company central offices (COs), it has not become widely 65 available until recently. Even now, it is usually available only in larger metropolitan areas. ISDN has not been as widely adopted as was once hoped. It has been eclipsed by xDSL and other connection types. ISDN comes in two basic forms: the Basic Rate Interface (BRI) and the Primary Rate Interface (PRI). The ISDN-BRI connection is made up of three channels. Two channels are called bearer channels and carry data at speeds of 64 Kbps per channel. Bearer channels can also carry voice calls—that is, spoken telephone calls. (Each bearer channel can carry one voice call at a time.) The third channel, called a data channel, carries call setup information and other overhead communications necessary to manage the two bearer channels. The data channel carries 16 Kbps of data. Bearer channels are abbreviated as B-channels; the data channel is abbreviated as a D-channel. Thus, an ISDN-BRI connection is often called a 2B+D connection, which reflects the number and the type of channels it contains. An ISDN-PRI connection is made up of 24 Bchannels and one D-channel. A PRI connection can carry a total of 1.544 Mbps—the same amount as a T-1 line ISDN connections are usually formed as needed—they are switched. For a WAN link, you use ondemand ISDN routers at each end, which can “dial up” the other router when data is pending. Because ISDN has extremely fast call setup times, ISDN connections are formed much more quickly than POTS connections—usually in less than a second. NOTE Although many systems can also use the Internet for videoconferencing, most firms rely on ISDN as the mainstay connection type for these types of calls. If you are setting up a video conferencing system, you should plan on installing at least two BRI connections (three is better) and purchase a videoconferencing system that supports at least 256 Kbps of bandwidth. Videoconferencing calls over a single BRI (128 Kbps) are fairly poor quality, two BRIs (256 Kbps) are much better, and three BRI (384 Kbps) connections are very good. Note also that both ends of a call need to support the same speed and number of BRIs ISDN pricing changes occur regularly. ISDN prices also vary considerably in different parts of the country. Getting full pricing information from your own regional Bell operating company (RBOC) before choosing ISDN is important. Then, using your projected usage data, you should be able to calculate the cost to use ISDN. Generally, the installation of an ISDN-BRI line, assuming no wiring changes is necessary, costs about $150. Some RBOCs might waive the installation charge if you sign an agreement to keep the ISDN line for one to two years. Monthly ISDN usage charges and longdistance ISDN call charges are similar to POTS charges. But remember that connecting with two Bchannels is equivalent to making two separate calls, and whatever charge exists for a single call will double when you use both B-channels.



Digital Subscriber Line (DSL)

The digital subscriber line (DSL) connection type has become widely available. A number of different flavors of DSL exist. Each of these types begins with a different initial or combination of initials, which is why DSL is often called xDSL. The available flavors include the following:

- ADSL Asymmetric DSL (ADSL) allows for up to 8 Mbps of data to be received and up to 1 Mbps of data to be sent. However, many RBOCs offer only up to 1.5 Mbps to be received (which is called the downstream direction) and 256 Kbps to be sent (called the upstream direction), and distance from the RBOC's local CO (the place where the RBOC equipment is located) might affect the speeds available at any particular location. At further distances, connections might be available only at much slower speeds (although in all cases, ADSL is still faster than POTS connections using a modem).

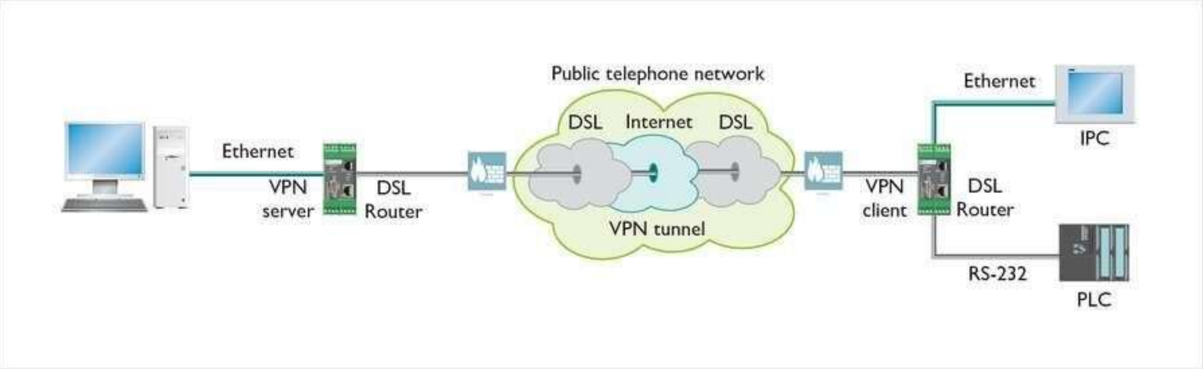
- HDSL High-speed DSL (HDSL) allows from 768 Kbps to 2.048 Mbps connections between two sites. HDSL is symmetric, meaning that the available upstream bandwidth and downstream bandwidth are the same.

- RADSL Rate-adaptive DSL (RADSL) allows for 600 Kbps to 12 Mbps of data to be received and 128 Kbps to 1 Mbps of data to be sent. RADSL is asymmetric.

- SDSL Symmetric DSL (SDSL) allows bidirectional rates varying from 160 Kbps to 2.048 Mbps.

- VDSL Very-high-speed DSL (VDSL) allows up to approximately 52 Mbps of bandwidth. VDSL can be either symmetric or asymmetric.

- IDSL ISDN-based DSL (IDSL) speed is about the same as ISDN. IDSL is used for data almost exclusively, because it's an always-on connection to a single destination (as discussed earlier, ISDN can be used to place calls to other ISDN connections) A lot of interest surrounds xDSL, particularly ADSL. The cost per megabyte of data transmitted is far less than POTS and is even considerably less expensive than ISDN. Presently, xDSL is available in most cities in the United States. In this section, you learn about how xDSL works and about when you might be able to implement its highbandwidth capabilities. This discussion focuses on ADSL because it is the most prevalent and the least expensive. For WAN links, however, you should consider SDSL if your WAN data needs are similar in both the downstream and upstream directions.



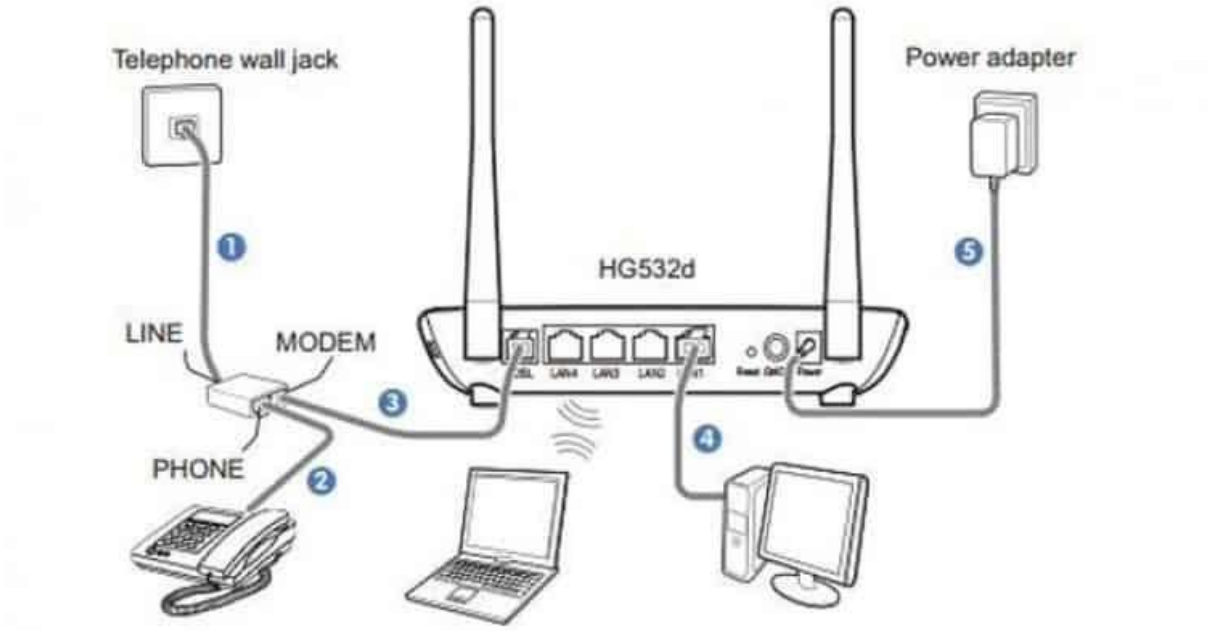
ADSL

ADSL works by using spectrum above the band used by voice telephone calls.[1] With a DSL filter, often called *splitter*, the frequency bands are isolated, permitting a single telephone line to be used for both ADSL service and telephone calls at the same time. ADSL is generally only installed for short distances from the telephone exchange (the last mile), typically less than 4 kilometres (2 mi),[2] but has been known to exceed 8 kilometres (5 mi) if the originally laid wire gauge allows for further[*clarification needed*] distribution.

At the telephone exchange, the line generally terminates at a digital subscriber line access multiplexer (DSLAM) where another frequency splitter separates the voice band signal for the conventional phone network. Data carried by the ADSL are typically routed over the telephone company's data network and eventually reach a conventional Internet Protocol network.

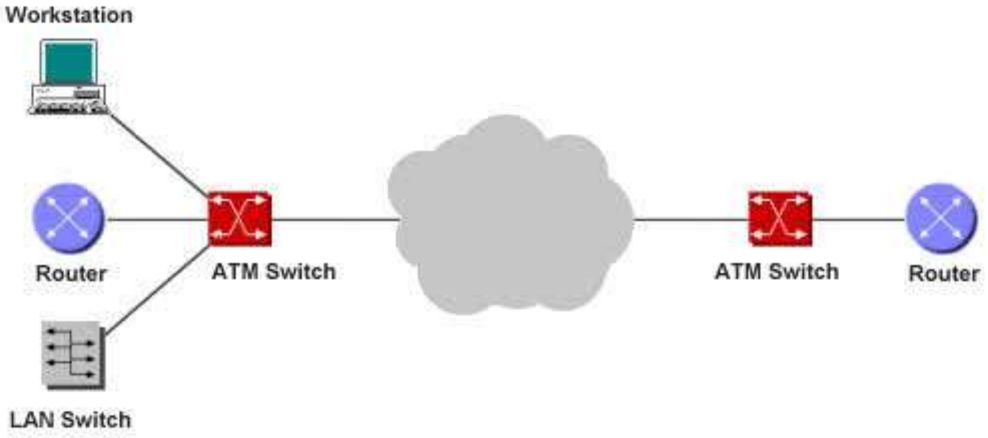
There are both technical and marketing reasons why ADSL is in many places the most common type offered to home users. On the technical side, there is likely to be more crosstalk from other circuits at the DSLAM end (where the wires from many local loops are close to each other) than at the customer premises. Thus the upload signal is weakest at the noisiest part of the local loop, while the download signal is strongest at the noisiest part of the local loop. It therefore makes technical sense to have the DSLAM transmit at a higher bit rate than does the modem on the customer end. Since the typical home user in fact does prefer a higher download speed, the telephone companies chose to make a virtue out of necessity, hence ADSL.

The marketing reasons for an asymmetric connection are that, firstly, most users of internet traffic will require less data to be uploaded than downloaded. For example, in normal web browsing, a user will visit a number of web sites and will need to download the data that comprises the web pages from the site, images, text, sound files etc. but they will only upload a small amount of data, as the only uploaded data is that used for the purpose of verifying the receipt of the downloaded data or any data inputted by the user into forms etc. This provides a justification for internet service providers to offer a more expensive service aimed at commercial users who host websites, and who therefore need a service which allows for as much data to be uploaded as downloaded. File sharing applications are an obvious exception to this situation. Secondly internet service providers, seeking to avoid overloading of their backbone connections, have traditionally tried to limit uses such as file sharing which generate a lot of uploads
https://en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line



Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode, commonly called just ATM, is a very high-speed technology for transmitting data between locations. ATM is a multiplexed, cell-based networking technology that collects data into entities called cells and then transmits the cells over the ATM network connection. ATM networks can carry both voice and data. ATM is very fast, with speeds ranging from 155 Mbps to 622 Mbps, and in some cases can go as high as 10 Gbps. Usually, ATM is used only by relatively large companies that need ATM's speed for their WAN links, or by companies that need to send enormous amounts of data through a network connection, such as a lot of video data.



STUDY UNIT SUMMARY

In this study unit, you learned about concepts and technologies relating to WANs, including different types of links and different types of connections, as well as how to specify a particular type of WAN technology for a given application. While the number of choices may make this area confusing, it becomes easier when you break the problem down into smaller chunks. Basically, make sure you do a careful and thorough job of identifying your WAN needs, and then work with various WAN providers in your area to analyze how their solutions may meet your needs. The next study unit moves into network protocols, like TCP/IP and IPX/SPX. You learn how these network protocols work, how their packets are constructed, and various characteristics of each type of network protocol. You also learn about some of the other common protocols, particularly those associated with TCP/IP, such as SMTP, HTTP, and WINS.

5.1.6 Revision Questions

Answer the compulsory revision questions below.

1. What is the difference between a switched and a dedicated WAN?
2. What is the difference between a private and public network?
3. What do you understand by dropped packets in a router?
4. In networking, what is latency related to?
5. How is ISDN different from DSL

` https://www.youtube.com/watch?v=9WkZT0YMZ70

https://www.youtube.com/watch?v=fCxfp1iUbqw

11. UNDERSTANDING NETWORKING PROTOCOLS

Purpose	The purpose of this unit is for the learner to be able to have in depth knowledge on how protocols govern network communication.
Learning Outcomes	By the end of this unit, you will be able to: • Explain and identify common protocols • Understanding Other Internet Protocols • Comparing Important Proprietary Protocols
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• TCP/IP • UDP • IPX/SPX • DNS • DHCP

5.6.1 INTRODUCTION

A network protocol is a set of rules that data communications over a network follow to complete various network transactions. For example, TCP/IP defines a set of rules used to send data from one node on a network to another node. SMTP is a set of rules and standards used to transfer email and attachments from one node to another. DHCP is a set of rules and standards used to allocate IP addresses dynamically for a network, so they do not need to be set manually for each workstation. Many protocols are used in networking. In fact, in a sense, almost every activity on a network follows a protocol of one sort or another. Some protocols function at a low level in the OSI network model, others operate at a high level, and some operate in between. In this study unit, you learn about the essential networking protocols used to transmit and receive data across a network.

Understanding TCP/IP and UDP

As its name suggests, TCP/IP is actually two protocols used in concert with one another. The Internet Protocol (IP) defines how network data is addressed from a source to a destination and in what sequence the data should be reassembled at the other end. IP operates at the network layer in the OSI model. The Transmission Control Protocol (TCP) operates one layer higher than IP, at the transport layer. TCP manages connections between computers. TCP messages are carried (encapsulated) in IP datagrams. The User Datagram Protocol (UDP) serves the same role as TCP but offers fewer features. Both TCP and UDP packets are carried within IP packets, but the only reliability feature that UDP supports is the resending of any packets not received at the destination. (UDP is called a connectionless protocol.) The chief advantage to UDP is that it is much faster for trivial network communications, such as sending a web page to a client computer. Because UDP doesn’t offer many error-checking or errorhandling features, it should be used only when it isn’t that important if data occasionally gets mangled between points and needs to be resent, or when an application program provides its own extensive error-checking and error-handling functions.

TCP and UDP Ports

Both TCP and UDP support the concept of ports, or application-specific addresses, to which packets are directed on any given receiving machine. For example, most web servers run on a server machine and receive requests through port 80. When a machine receives any packets that are intended for the web server (such as a request to serve up a web page), the requesting machine directs those packets to that port number. When you request a web page from a web server, your computer sends the request to the web server computer and specifies that its request should go to port 80, which is where HTTP requests are directed. Hundreds of different ports have standardized uses. Defining your own ports on a server for specific applications is easy. A text file called SERVICES defines the ports on a computer. An example of a portion of a Windows SERVICES file follows. (Only selected entries are shown due to space constraints; the following is not a complete SERVICES file, but it illustrates what the file contains.)

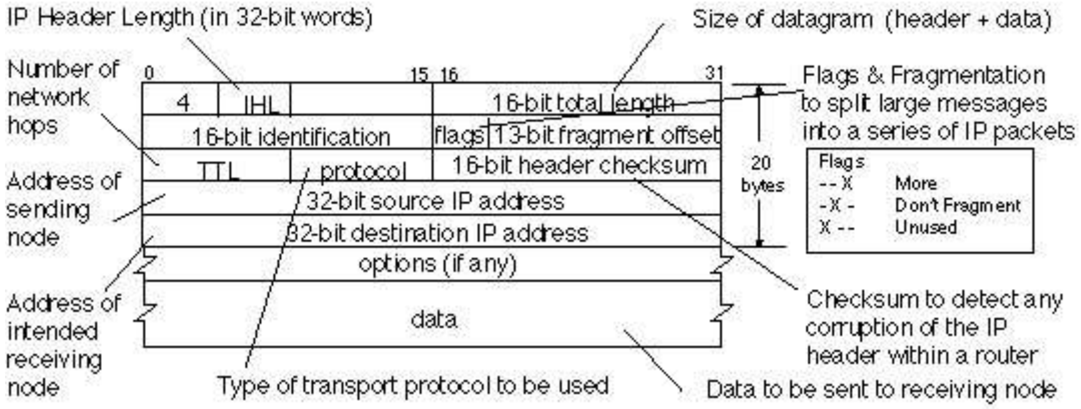
As you can see, most of the Internet services that you might be familiar with actually work through the use of TCP and/or UDP ports, such as HTTP for the Web, SMTP for e-mail, NNTP for Usenet, and so forth. The use of ports ensures that network communications intended for a particular purpose are not confused with others that might also be arriving at the same machine. Ports allow the receiving machine to direct arriving data appropriately. An example is a server that hosts web pages and also receives and processes e-mail. Packets arriving at port 80 will be sent to the web-serving software, while those that arrive at port 25 will go to the e-mail software. Other services on the machine, such as Telnet and FTP, can also function concurrently through this mechanism.

IP Packets and IP Addressing

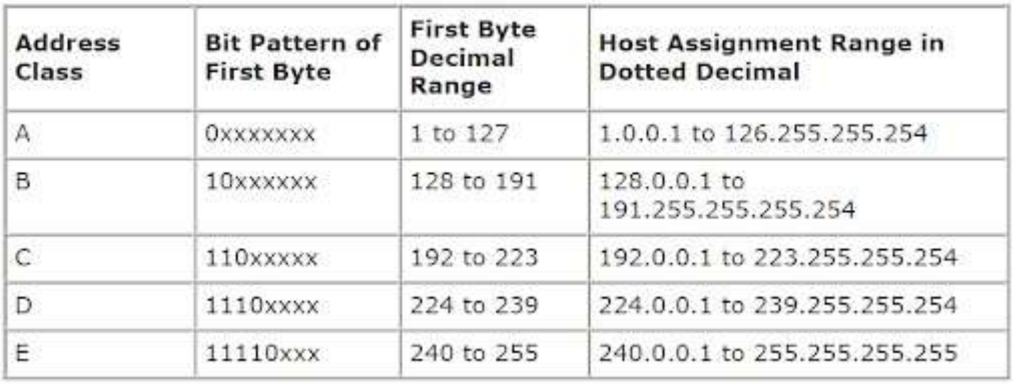
IP packets include addresses that uniquely define every computer connected to the Internet . These addresses are used to route packets from a sending node to a receiving node. Because all the routers on the Internet know the network addresses to which they are connected, they can accurately forward packets destined for a remote network.

In addition to carrying its data, each IP packet contains a number of fields, which are organized in the following order:

- Version This field indicates the version of the IP protocol being used.
- Header length This field indicates the length of the header information before the data begins in the packet.
- Type of service This field is used for different purposes by different vendors. It can be used for features such as requesting high-priority routing, requesting highest possible reliability, and so forth.
- Total length This field indicates the total length of the packet.
- Identification, flags, and fragment offset These three fields are used to reassemble an IP packet that was disassembled at some point during transmission. They include all the information necessary for the correct reassembly of the packet at the receiving end.
- Time to live This field defines how many network hops the packet can traverse before it is declared dead and the routers stop forwarding it to other routers. This number is set when the packet is sent, and each router that handles the packet decrements the value by one. When the number reaches zero, the packet is dead and is no longer transmitted. If there is a routing configuration error on the path to the destination that causes the packet to go into an endless loop between routers, this is the feature that will stop it after a period of time.
- Protocol This field indicates whether the IP packet is contained within a TCP or a UDP packet.
- Header checksum The header checksum is used to help ensure that none of the packet’s header data (the fields discussed in this list) is damaged.
- Source IP address this field contains the address of the sending computer. It is needed in case a packet must be retransmitted, to tell the receiving node (or, in some cases, a router) from which node to request a retransmission.
- Destination IP address this field contains the address of the receiving node.
- Options and padding these final two fields of the header of the IP packet are used to request any required specific routing instructions or to specify the time that the packet was sent.
- Data The final field of an IP packet is the actual data being sent. IP addresses are 32 bits long, allowing for a theoretical maximum number of addresses of 232, or about 4.3 billion addresses. To make them easier to work with and to help route them more efficiently, they are broken up into four octets, which are each 1 byte long. Thus, in decimal notation, IP addresses are expressed as xxx.xxx.xxx.xxx, where each xxx represents a base-10 number from 0 to 255. The numbers 0, 127, and 255 are usually reserved for special purposes, so they are typically unavailable for assignment to nodes. The remaining 253 unique addresses are available for assignment in each octet.

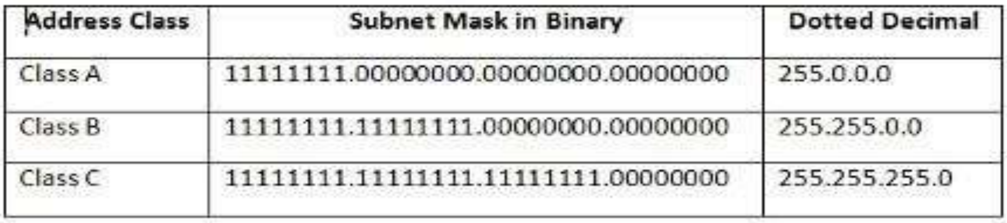

IP Header Length (in 32-bit words)
Size of datagram (header + data)
Number of network hops
0
15 16
31
4
IHL
16-bit total length
16-bit identification
flags
13-bit fragment offset
TTL
protocol
16-bit header checksum
32-bit source IP address
32-bit destination IP address
options (if any)
data
20 bytes
Flags & Fragmentation to split large messages into a series of IP packets
Flags
-- X More
-X - Don't Fragment
X -- Unused
Address of sending node
Address of intended receiving node
Checksum to detect any corruption of the IP header within a router
Type of transport protocol to be used
Data to be sent to receiving node

Addresses on the Internet are guaranteed to be unique through the use of an address registration service, presently administered by the Internet Corporation for Assigned Names and Numbers (ICANN). Actual registrations of domain names and addresses are handled through one of many registrars, which include companies such as InterNIC, Network Solutions, and many others. ICANN is the overall authority. ICANN assigns three major classes of addresses, called Class A, B, and C, as follows:



Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

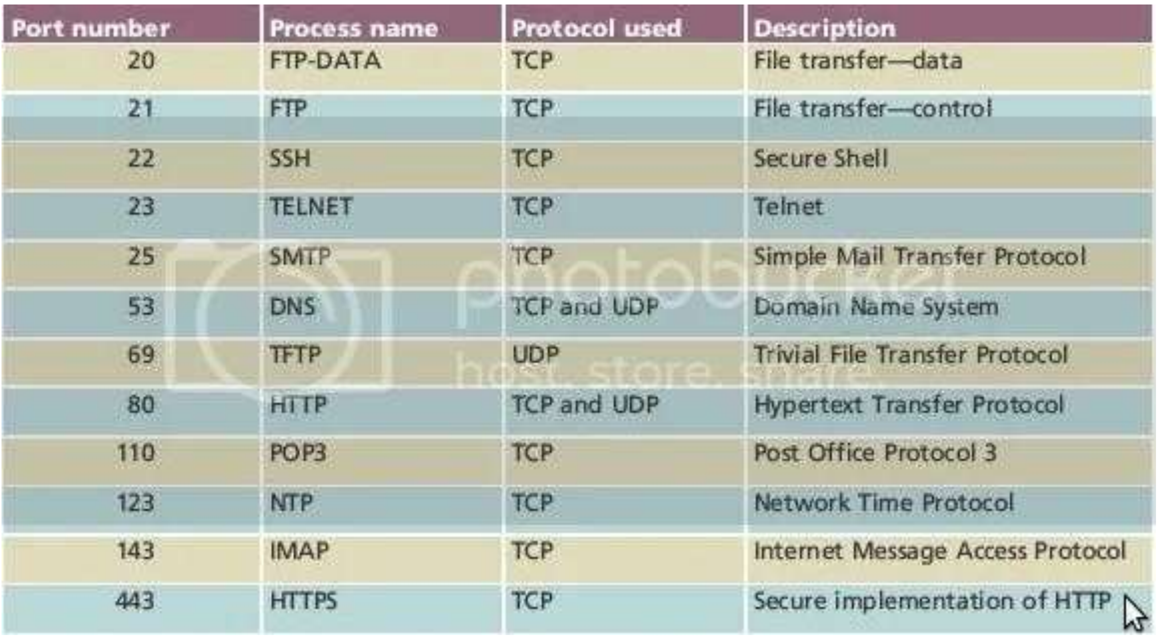
Subnet Masks



Address Class	Subnet Mask in Binary	Dotted Decimal
Class A	11111111.00000000.00000000.00000000	255.0.0.0
Class B	11111111.11111111.00000000.00000000	255.255.0.0
Class C	11111111.11111111.11111111.00000000	255.255.255.0

Understanding Other Internet Protocols

Quite a few other protocols used on the Internet either rely on or make use of TCP/IP. In this section, you learn about these different protocols.



Port number	Process name	Protocol used	Description
20	FTP-DATA	TCP	File transfer—data
21	FTP	TCP	File transfer—control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP and UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP and UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

Voice over IP (VoIP)

VOIP is an acronym for Voice Over Internet Protocol, or in more common terms phone service over the Internet.
If you have a reasonable quality Internet connection you can get phone service delivered through your Internet connection instead of from your local phone company.

Some people use VOIP in addition to their traditional phone service, since VOIP service providers usually offer lower rates than traditional phone companies, but sometimes doesn’t offer 911 service, phone directory listings, 411 service, or other common phone services. While many VoIP providers offer these services, consistent industry-wide means of offering these are still developing.

There are two major reasons to use VOIP

- Lower Cost
- Increased functionality

  - **Lower Cost**

In general phone service via VOIP costs less than equivalent service from traditional sources. This is largely a function of traditional phone services either being monopolies or government entities. There are also some cost savings due to using a single network to carry voice and data. This is especially true when users have existing under-utilized network capacity that they can use for VOIP without any additional costs.

In the most extreme case, users see VOIP phone calls (even international) as FREE. While there is a cost for their Internet service, using VOIP over this service may not involve any extra charges, so the users view the calls as free. There are a number of services that have sprung up to facilitate this type of “free” VOIP call. Examples are: Free World Dialup and Skype for a more complete list see: VOIP Service Providers

- **Increased Functionality**

VOIP makes easy some things that are difficult to impossible with traditional phone networks.

- Incoming phone calls are automatically routed to your VOIP phone where ever you plug it into the network. Take your VOIP phone with you on a trip, and anywhere you connect it to the Internet, you can receive your incoming calls.

- Call center agents using VOIP phones can easily work from anywhere with a good Internet connection.

https://www.voip-info.org/what-is-voip/?__cf_chl_jschl_tk__=41e7735f1a4f4c8cde10f66df226ccaa23c528e1-1609916427-0AazsxcqJ2GqQkMAuIL6f1pg2_IHsgMoEpWzhEzGvMc1hivvD6NYHLYBN1WtAXLZUmTTBpRTw5G9hX3iu4GuRZwOcqHQRXI4UqNLKhKcLl4y4rniORGVHqGCVNcmOe0JwAiXdvWzG5mamzaNxO6h63j5hZgeu4ZDwBqdjNU8aVRfygZSjXAhfhMvTfd1E12q9QIBpGIEt0Kk5ccZktLCJud07nZrFTwamsigcfjwoN28pzOyri_8qp0niG0z6YuvJPKo7iCN-zzePjN8q0r66t-Ma9ncEwhcIwUdPu5Mt2lArqpDkl-5bMhO0yiFugwO1zygUp_ynjYHGmfQtvhMoKX3_DaLXhzbj1iSieQPZIgyHdbDsaYEYbETycRlyQeKTeg

VoIP also has some disadvantages that you need to consider:

- **No guaranteed delivery**:

VoIP does not guarantee delivery of IP packets over the Internet. For a digital transmission of data, this is no big deal; if a packet isn’t confirmed as being received, it is simply retransmitted. For a realtime voice conversation, the loss of packets directly inhibits the conversation, and you can’t go back in time to retransmit missing packets.

- **Out-of-sequence packets**

Not only can IP packets simply fail to arrive at their destination on occasion, but sometimes they arrive out of sequence due to other Internet traffic and other reasons. This is fine for transmitting things such as files, because the packets can be reassembled on the other end in the proper sequence once they are all received. For a real-time application such as voice, however, having packets arrive out of sequence results in a hopelessly jumbled, and thus useless, transmission.

- **QoS not widely implemented**

Real-time uses of the Internet, such as VoIP or multimedia streaming and time-sensitive transmissions, should be given priority over transmissions that are not particularly time-sensitive, such as the transmission of an e-mail message. Fortunately, IP has a quality of service (QoS) field that enables the user to prioritize traffic for such reasons. However, QoS is not widely implemented in all parts of the Internet.

AppleTalk

AppleTalk is a set of proprietary networking protocols developed by Apple for their computer systems. AppleTalk was included in the original Macintosh released in 1984. In 2009, it became unsupported with the release of Mac OS X v10.6 and was dropped in favor of TCP/IP networking, allowing Apple computers to use the same standard to communicate with other computers.

The design of AppleTalk followed the OSI Model of protocol layering with two protocols aimed at making the system completely self-configuring:

- AppleTalk Address Resolution Protocol (AARP): Allowed hosts to automaticall generate their own network addresses
- Name Binding Protocol (NBP): A dynamic system that maps network addresses to userreadable names.

AppleTalk was revolutionary and easy to configure in its day. However, with the rise of Internetbased protocols and their standardization, the need for a proprietary system quickly declined. If Apple had not conformed to other standards, they were in danger of losing the competition. Hence, they finally dropped AppleTalk in favor of TCP/IP. Apple supported AppleTalk for older devices for a while. However, the last Mac OS to support AppleTalk was OS X v10.5.

AppleTalk used a 4-byte address system and used completely self-configuring protocols. The address resolution protocol allowed hosts to generate their own address automatically. The name binding protocol allowed the system to dynamically map the network address to user-readable names of terminals.

An AppleTalk address consisted of a two-byte network number, a one-byte node number, and a onebyte socket number. Only the network number needed configuration, which was obtained from a router. This allowed for a total of 32 devices to be connected to the network and operated at 230.4 KBps with the devices being up to 1000 feet apart.

https://www.techopedia.com/definition/2631/appletalk

STUDY UNIT SUMMARY

This study unit is built on the knowledge you gained in earlier study units, delving into various important protocols involved in virtually all networks, including the Internet. You learned primarily about the TCP/IP protocol, which has essentially displaced older protocols such as 84 IPX/SPX and NetBIOS/NetBEUI (although these older protocols are still used). You also learned about some specific application-layer Internet protocols, such as SMTP, DHCP, and HTTP. These are all vital protocols to understand for any networking professional. It would be nice if the protocols discussed in this study unit were all you had to contend with, but, unfortunately, many more protocols exist. Some are specific to certain functions, such as remote access to a network, and are discussed in appropriate study units within this book. Others are still being developed and are not a factor now, but may be in the near future. You will certainly want to stay up-to-date with emerging protocols that may become important to networking. The next study unit is about directory services, which make complex networks easier to use and administer.

5.1.7 Revision Questions

Answer the compulsory revision questions below.

1. How many bits do an IPv4 and IPv6 have?
2. What protocol does Microsoft use for small networks?
3. Which is the best protocol used on the internet?
4. Which protocol did Microsoft create that was intended to be used on the internet? Which software is commonly used with VoIP?

https://www.youtube.com/watch?v=wvPe4Zb0tUA

https://www.youtube.com/watch?v=3b_TAYtzuho

12. EXPLORING DIRECTORY SERVICES

Purpose	The purpose of this unit is for the learner to be able to understand how directory service are essential in the runnings of an enterprise network.
Learning Outcomes	By the end of this unit, you will be able to: • Active directory • Domains, forests and trees • Other network directory services.
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• LDAP • DOMAINS • PDC AND BDC • X.500

5.7.1 INTRODUCTION

In the early days of local area networks (LANs), finding server resources was simple. Most organizations started with just a file server and a print server or two, so knowing which files, printers, and other services were in which locations on the LAN was easy. These days, the situation is considerably more complex. Even relatively small organizations might have multiple servers, all performing different jobs—storing different sets of files and providing different Internet or intranet services, such as e-mail servers, web hosting, database servers, network services, and so forth. Directory services work to bring organization to this far-flung network clutter. In this study unit, you learn about what directory services do and how they work. You also learn about the directory services in use today and those slated for use in the near future. With directory services becoming more and more central to the administration of networks, learning this information becomes an increasingly important part of designing, deploying, and managing networks.

What Is a Directory Service?

In most networks, you optimize the function of different services by hosting them on different computers. Doing so makes sense. Putting all your services on one computer is a bit like placing all your eggs in one basket—if you drop the basket, you'll break all your eggs. Moreover, you can achieve optimal performance, more reliability, and higher security by segregating network services in various ways. Most networks have quite a few services that need to be provided, and often these services run on different servers. Even a relatively simple network now offers the following services:

- File storage and sharing
- Printer sharing
- E-mail services
- Web hosting, both for the Internet and an intranet
- Database server services
- Specific application servers
- Internet connectivity
- Dial-in and dial-out services
- Fax services
- Domain Name System (DNS) service, Windows Internet Naming Service (WINS), and Dynamic Host Configuration Protocol (DHCP) services
- Centralized virus-detection services
- Backup and restore services

This is only a short list. Larger organizations have multiple servers sharing in each of these functions— with different services available through different means in each building or location—and might have additional services beyond those listed here. All this complexity can quickly make a network chaotic to manage. If each one of the individual servers required separate administration (with, for instance, separate lists of users, passwords, groups, printers, network configurations, and so on), the job would become virtually impossible in no time.

Directory services were invented to bring organization to networks. Basically, directory services work just like a phone book. Instead of using a name to look up an address and phone number in a phone book, you query the directory service for a service name (such as the name of a network folder or a printer), and the directory service tells you where the service is located. You can also query directory services by property. For instance, if you query the directory service for all items that are "printers," it can return a complete list, no matter where the printers are located in the organization. Even better, directory services enable you to browse all the resources on a network easily, in one unified list organized in a tree structure.

One important advantage of directory services is that they eliminate the need to manage duplicates of anything on the network because the directory is automatically shared among all of the servers. For example, you don't need to maintain separate user lists on each server. Instead, you manage a single set of user accounts that exists in the directory service and then assign them various permissions to particular resources on any of the servers. Other resources work the same way and become centrally managed in the directory service. Not only does this mean that you have only one collection of objects to manage, but also that users have a much simpler network experience. From the users' perspective, they have only one network account with one password, and they don't need to worry about where resources are located or keep track of multiple passwords for different network services or servers. To provide redundancy, directory services usually run on multiple servers in an organization, with each of the servers having a complete copy of the entire directory service database. Because a directory service becomes central to the functioning of a network, this approach lets the network as a whole continue to operate if any single server with directory services on it crashes. Servers that do not actually host a copy of the directory still make use of it by communicating with the directory servers. For instance, if a user tries to open a file hosted on a server that doesn't actually host the directory service, the server will automatically query the directory service on another server to authenticate the user's access request. To the user, this happens behind the scenes. You should know about five important directory services: Novell eDirectory, Microsoft's Windows NT domains, Microsoft's Active Directory, X.500 Directory Access Protocol, and Lightweight Directory Access Protocol. These are described later in this study unit.

Active Directory

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts. For more information about the Active Directory data store, see Directory data store.

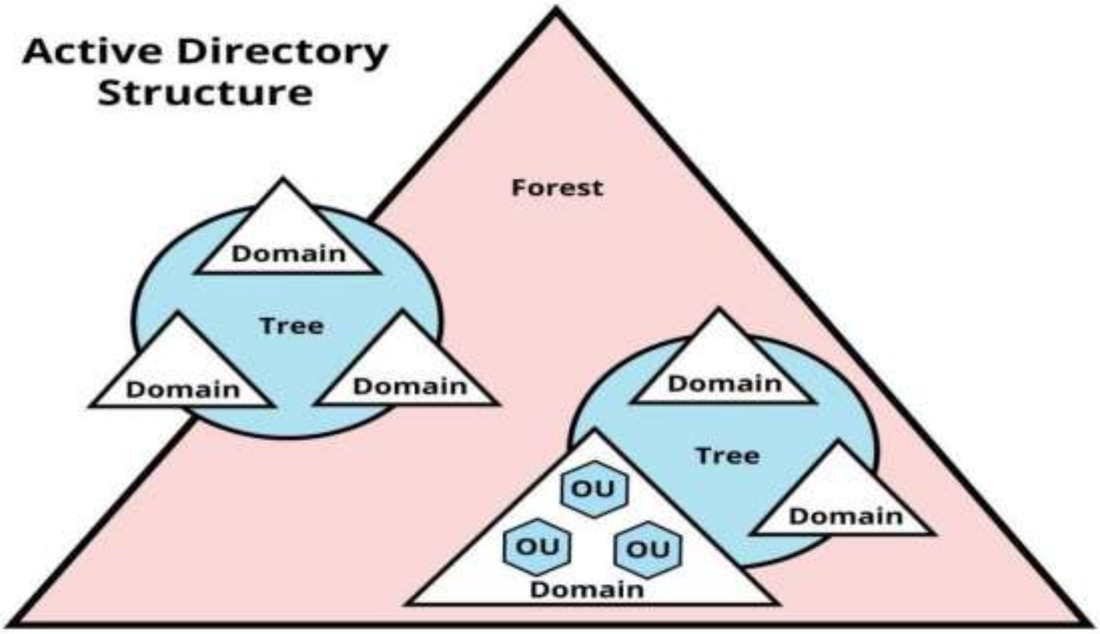
Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network. For more information about Active Directory security.

Active Directory also includes:

- A set of rules, **the schema**, that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names. For more information about the schema, see Schema.
- A **global catalog** that contains information about every object in the directory. This allows users and administrators to find directory information regardless of which domain in the directory actually contains the data. For more information about the global catalog, see The role of the global catalog.
- A **query and index mechanism**, so that objects and their properties can be published and found by network users or applications. For more information about querying the directory, see Finding directory information.
- A **replication service** that distributes directory data across a network. All domain controllers in a domain participate in replication and contain a complete copy of all directory information for their domain. Any change to directory data is replicated to all domain controllers in the domain. For more information about Active Directory replication, see Replication overview.

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/activedirectory-domain-services-overview

Active Directory Structure



X.500

The X.500 standard was developed jointly by the International Telecommunications Union (ITU) and the International Standards Organization (ISO). The standard defines a directory service that can be used for the entire Internet. Because of its broad applicability, the X.500 specification is too complex for most organizations to implement. Also, because of its design, it is intended to publish specific organizational directory entries across the Internet, which is something most companies would not want to do. Just the same, the X.500 standard is extremely important, and most directory services mimic or incorporate parts of it in some fashion. The X.500 directory tree starts with a root, just like the other directory trees, and then breaks down into country (C), organization (O), organizational unit (OU), and common name (CN) fields. To specify an X.500 address fully, you provide five fields, as in the following:

CN=user name, OU=department, OU=division, O=organization, C=country

For example, you might configure the fields as follows:

CN=Bruce Hallberg, OU=Networking Books, OU=Computer Books, O=McGraw-Hill,

C=USA

LDAP

To address the complexity problems involved with full X.500 DAP, a consortium of companies came up with a subset of X.500, called LDAP. LDAP's advocates claim that it provides 90 percent of the power of X.500, but at only 10 percent of the processing cost. LDAP runs over TCP/IP and uses a client/server model. Its organization is much the same as that of X.500, but with fewer fields and fewer functions. LDAP is covered predominantly by RFC 1777 (for version 2) and RFC 2251 (for version 3). (Some other RFCs also describe aspects of LDAP.) The LDAP standard describes not only the layout and fields within an LDAP directory, but also the methods to be used when a person logs in to a server that uses LDAP, or queries or updates the LDAP directory information on an LDAP server. (Because directory services might fulfill many simultaneous authentications, run simultaneous queries, and accept simultaneous updates, it is important that these methods be clearly defined to avoid collisions and other potentially corrupting uses of the directory by client applications and administrative tools.) An LDAP tree starts with a root, which then contains entries. Each entry can have one or more attributes. Each of these attributes has both a type and values associated with it. One example is the CN ("common name"), which contains at least two attributes: FirstName and Surname. All attributes in LDAP use the text string data type. Entries are organized into a tree and managed geographically and then within each organization.

The following four basic models describe the LDAP protocol:

- Information model this model defines the structure of the data stored in the directory. It describes a number of aspects of the directory, including the schema, classes, attributes, attribute syntax, and entries. The directory's schema is the template for the directory and its entries. Classes are categories to which all entries are attached. Attributes are items of data that describe the classes, such as CN and OU. The syntax for the attributes specifies exactly how attributes are named and stored, and what sort of data they are allowed to contain (such as numbers, string text, dates and times, and so forth). Finally, entries are distinct pieces of data; like objects, that can be either a container or a leaf.

- Naming model this model describes how to reference and organize the data. It defines the names that serve as primary keys for entries in the directory: Distinguished names (DNs), which are full names of entries, as well as relative distinguished names (RDNs), which are components of DNs. Each component of the DN—such as the CD, OU, or O entries— is an RDN. The following is an example of an LDAP DN: CN=Bruce Hallberg, OU=Networking Books, OU=Computer Books, O=McGraw-Hill, C=USA.

- Functional model this model describes how to work with the data. It defines how LDAP accomplishes three types of operations: authentication, interrogation, and updates. Authentication is the process by which users prove their identity to the directory. Interrogation is the process by which the information in the directory is queried. Updates are operations that post changes to the directory.

- Security model this model defines how to keep the data in the directory secure. For most implementations of LDAP, a security protocol called Simple Authentication and Security Layer (SASL) is used. RFC 2222 describes SASL.

STUDY UNIT SUMMARY

In this study unit, you learned about both the importance of directory services and the factors driving that importance. You also learned how directory services work, what they accomplish, and those common features found in almost all directory services. Finally, the most important directory services were each reviewed, including Novell's eDirectory, Microsoft's domain service, and Active Directory service.

5.1.8 Revision Questions

Answer the compulsory revision questions below.

1. Why is directory service important in a enterprise network?
2. State 4 services provided by a directory?
3. Describe the active directory structure?
4. Which protocol is usually associated with directory services?

https://www.youtube.com/watch?v=qkN4bvqWqvo

https://www.youtube.com/watch?v=QyhNaY5O468

13. REMOTE NETWORK ACCESS

Purpose	The purpose of this unit is for the learner to be able to understand how remote connectivity is established and maintained
Learning Outcomes	By the end of this unit, you will be able to: • What Types of Remote Users Do You Need to Support? • Understanding Application Implications for Remote Access • Determining Remote Access Needs • What Types of Remote Users Do You Need to Support?
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• PPP • PPTP • SLIP

5.8.1 INTRODUCTION

In the preceding study units, you learned about networking systems together through a local area network (LAN) and through a wide area network (WAN), and about the technologies that go into both types of networks. You also need to know about another important type of network connection: remote access to a network. With today's travel-happy corporate cultures, and with companies needing to support such things as working from home and small remote offices, remote access has become more important than ever. Unfortunately, it's also one of the most difficult parts of a network to get right, as you will see in this study unit.

One of the big problems with remote access is that it can seem as though all the remote users have different requirements, the various solutions address different needs, and none of those solutions takes care of all the needs. Finding solid solutions that meet those needs is usually nontrivial and requires a fair amount of time and effort. This study unit describes how you might analyze your company's needs and then discusses the remote access technologies that can provide a solution (or solutions) for your network.

UNDERSTANDING APPLICATION IMPLICATIONS FOR REMOTE ACCESS

Client/server applications consist of processes (programs) that run on both the server side and the client side, and work in concert. For example, a database server performs queries for the client, and then transmits to the client only the results of that query. The client's job is just to display the results and maybe format them for printing. A monolithic application, on the other hand, performs all of its work on one computer, typically the client computer. The server for a monolithic application serves up only the files needed for the application to run and the data files that the application manipulates. Generally, client/server applications require much less bandwidth to work at acceptable speeds than monolithic applications. A slow network connection might be adequate for a client/server application, such as an accounting system, whereas that connection would be totally inadequate for that same application designed to be monolithic.

What Types of Remote Users Do You Need to Support?

Users who require remote access generally fall into one of the following four categories:

- Broad traveler
- Narrow traveler
- Remote office user
- Remote office group Each category of remote user has different needs, and different technologies and remote access solutions are often required to satisfy these needs completely.

Your first step in finding a remote access solution is to determine which categories of remote users you must support. So, let's look at each of these remote access user categories. The broad traveler is the most common type of remote access user. This is someone who normally is based in an office that has LAN access, but also travels on business. Travel takes this person to virtually any place in the world, so the traveler must contend with different telephone systems, long-distance carriers, and other geographic challenges.

Often, this type of user mostly needs e-mail access, with occasional access to stored or e-mailed files. The user might normally use a desktop computer on the LAN but have a laptop computer for traveling, might use a single laptop both on the LAN and when traveling, might check out laptop computers from a shared pool when travel needs arise, or might even rent a laptop computer for an occasional travel need. These different approaches further complicate providing services to the broad traveler.

REMOTE ACCESS CONNECTION CONFIGURATION REQUIREMENTS

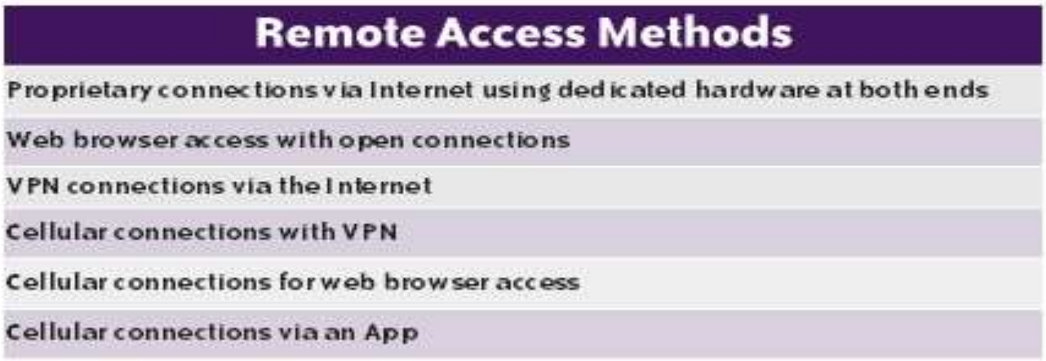
- Access Methods The rules governing the use of physical network by various devices are called Access Methods. Each networking topology has its own access method so that it data can be successfully transmitted. Even though there may be numerous devices contending for use at any given time. Most clients are connected directly to the network. Microsoft provides Remote Access Service (RAS) to let you set up and configure client access. Users connecting to a RAS service can be limited to access the server and allowing only one user access to the network. It is important to select connection options appropriate to your access requirements You can select from the following:-

- Modem

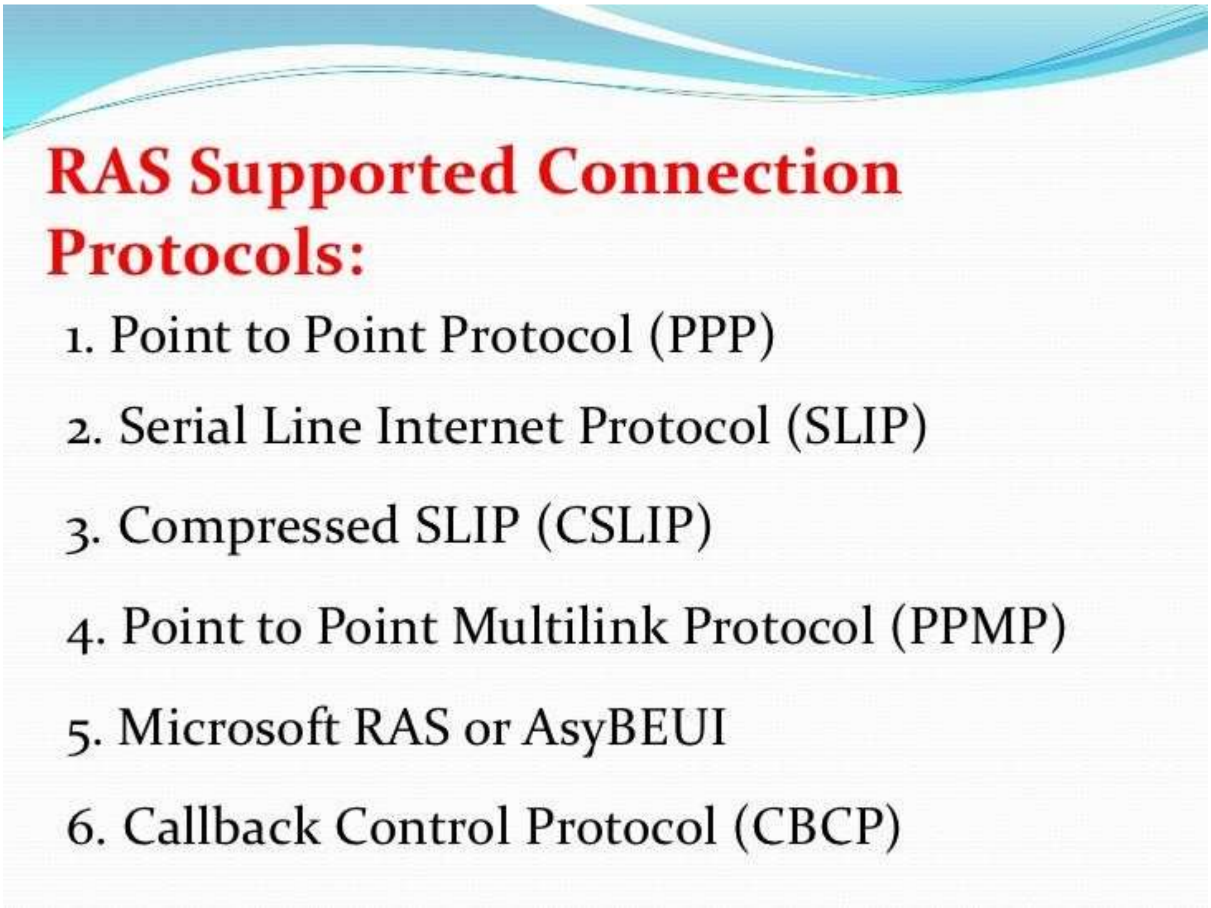
- Null Modem

- ISDN

REMOTE ACCESS CONNECTION METHODS



Remote Access Methods
Proprietary connections via Internet using dedicated hardware at both ends
Web browser access with open connections
VPN connections via the Internet
Cellular connections with VPN
Cellular connections for web browser access
Cellular connections via an App



RAS Supported Connection Protocols:

1. Point to Point Protocol (PPP)
2. Serial Line Internet Protocol (SLIP)
3. Compressed SLIP (CSLIP)
4. Point to Point Multilink Protocol (PPMP)
5. Microsoft RAS or AsyBEUI
6. Callback Control Protocol (CBCP)

STUDY UNIT SUMMARY

Most network administrators would agree that supporting remote access is one of the trickiest parts of managing any network. Many factors come together to make this so. You can support remote connections in a number of ways. Most remote connection speeds have lower bandwidth than remote users would like. Many remote users are often important people in the company. Still, remote access is an important network service, and its benefits to the company justify most levels of effort to make it reliable and work right.

5.1.9 Revision Questions

Answer the compulsory revision questions below.

1. Explain the concept of remote access 2.
What do you understand by bandwidth?
3. Differentiate between Remote Node and Remote Control
4. What is VPN
5. Name four types of VPN

https://www.youtube.com/watch?v=34ldGdtlvmk

14. NETWORK SECURITY

Purpose	The purpose of this unit is for the learner to be able to understand how security of networks is pivotile in any enterprise.
Learning Outcomes	By the end of this unit, you will be able to: • Understanding Internal Security • Practices and User Education • Understanding External Threats • Viruses and Other Malicious Software
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• DDOS • MALWARE • VIRUS

5.9.1 INTRODUCTION

Most networking tasks are relatively straightforward. Do you want a new file and print server? You install it and set it up, and it either works or it doesn't. If it doesn't work, you proceed to troubleshoot it, fix any issues, and ultimately complete the task. Network security, on the other hand, is a horse of a different color. You can never really finish the project of securing a network, and you can never be certain that a network is completely secure. How much money you invest in securing a network, how much time you devote to the job and how much fancy security hardware and software you install doesn't matter—no network is ever completely secure. Having said that, network security is one of the most important jobs facing any network administrator. Good network security helps prevent the following:

- Company secrets, such as proprietary designs or processes, falling into the wrong hands (both internally and externally)
- Personal information about employees falling into the wrong hands

- Loss of important information and software
- Loss of use of the network itself or any part of the network
- Corruption or inappropriate modification of important data

These are just some of the more important losses that network security can prevent. If you spend any time thinking about all the information that is stored on and that flows through networks with which you work (and you should spend time thinking about this), you'll probably come up with additional dangers to avoid. This study unit provides an overview of the subject of network security. Its aim is to familiarize you with important network security ideas and concepts, as well as various technologies involved in network security. If you are responsible for a network's security, you should pursue more detailed information, and you should also seriously consider hiring a specialist on this subject to help you secure your network. Even if you don't have primary responsibility to keep your network secure, the security of the network is everyone's job. If you're an IT professional, security is an even more important part of your job.

Understanding Internal Security

Internal security is the process of securing your network from internal threats, which are generally much more common than external threats. Examples of internal threats include the following:

- Internal users inappropriately accessing information such as payroll records, accounting records, or business development information.
- Internal users accessing other users' files to which they should not have access.
- Internal users impersonating other users and causing mischief, such as sending e-mail under another person's name.
- Internal users accessing systems to carry out criminal activities, such as embezzling funds.
- Internal users compromising the security of the network, such as by accidentally (or deliberately) introducing viruses to the network. (Viruses are discussed in their own section later in this study unit.)
- Internal users "sniffing" packets on the network to discover user accounts and passwords.

To deal with threats such as these, you need to manage the network's security diligently. You should assume that, in the population of internal users, at least some exist who have the requisite sophistication to explore security holes in the network and that at least a few of those might, at some point, try to do so.

Account Security

Account security refers to the process of managing the user accounts enabled on the network. A number of tasks are required to manage user accounts properly, and the accounts should be periodically audited (preferably by a different person than the one who manages them daily) to ensure that no holes exist. Following are a number of general steps you should take to manage general account security:

- Most network operating systems start up with a user account called Guest. You should remove this account immediately, because it is the frequent target of crackers (a hacker is a person who likes to explore and understand systems, while a cracker is a person who breaks into systems with malicious intent). You should also avoid creating accounts that are obviously for testing purposes, such as Test, Generic, and so forth.

- Most network operating systems start up with a default name for the administrative account. Under Windows server operating systems, the account is called Administrator; under NetWare, it is called either Supervisor or Admin (depending on which version you are using). You should immediately rename this account to avoid directed attacks against the account. (Under NetWare 3.x, you cannot rename the Supervisor account.)

- You should know the steps required to remove access to network resources quickly from any user account and be sure to explore all network resources that might contain their own security systems. For example, accounts will be managed on the network operating system (and possibly on each server) and also in specific applications, such as database servers or accounting systems. Make sure that you find out how the system handles removed or deactivated accounts. If you delete a user account in order to remove access, some systems don't actually deny access to that user until they log out from the system.

- Work closely with the human resources (HR) department. Make sure that the HR staff is comfortable working with you on handling security issues related to employee departures, and develop a checklist to use for standard employment changes that affect IT. The HR department might not be able to give you much—if any—advance notice, but it needs to understand that you need to know about any terminations immediately, so you can take proper steps. Along the same lines, you should develop a set of procedures on how you handle accumulated e-mail, files, and other user access—both for friendly departures and terminations. Your relationship with the appropriate people in the HR department is crucial in being able to handle security well, so make sure that you establish and maintain mutual trust.

- Consider setting up a program whereby new users on the network have their assigned permissions reviewed and signed off by their supervisor. This way, you won't mistakenly give people access to things they shouldn't have.

- For publicly traded companies, the advent of the Sarbanes-Oxley Act of 2002 (discussed in Study unit1) means you will likely need to set up a system to document how users of the network are added, modified, and removed from the system. This type of system usually involves a set of request forms initiated by the appropriate department (HR, accounting, and so on), signed by the individual's supervisor and any other parties that need to authorize access to certain systems, and then documents the IT staff's actions. These forms are then filed and will be examined by the company's auditors.

Password Security

Another important aspect of account security is account password security. Most network operating systems enable you to set policies related to password security. These policies control how often the system forces users to change their passwords, how long their passwords must be, the complexity of the password (alphanumeric, capital letters, or symbols), whether users can reuse previously used passwords, and so forth. At a minimum, consider these suggestions for password policies:

- Require users (through network password policy settings) to change their main network password every 90 to 180 days. (Actually, 30 days is a common recommendation, but this might be too frequent in most environments.)
- Set the reuse policy so that passwords cannot be reused for at least a year.
- Require passwords that are at least eight characters long. For case-insensitive passwords that do not allow special characters, this yields potentially 368 possible permutations, or almost 3 trillion possibilities. And if the network operating system uses case-sensitive passwords, the possibilities are much larger: 628 (218 trillion). For systems that allow special characters to be part of the password (characters like a space, comma, period, asterisk, and so forth), the number of possible combinations is even higher still.
- Encourage users to create passwords that are not words in any language or, if they are words, that they have numbers and other non-alphanumeric characters inserted somewhere in the word, so a "dictionary attack" won't easily work. (Many password-cracking programs rely on dictionaries of

common words and names to reduce dramatically the number of possibilities 103 they need to try.) Also, for networks that support mixed-case passwords encourage users to use mixed-case characters.

- Make sure that you turn on any policies that monitor for and deal with people entering in wrong passwords. Often called intruder detection, this type of policy watches for incorrect password attempts. If too many attempts occur within a set period of time, the system can lock out the user account, preventing further attempts. I usually set this type of feature to lock an account any time five incorrect passwords are entered within an hour, and then lock the account until its reset by the administrator. This way, if users enter a large number of incorrect passwords, they will need to talk with the administrator to reopen the account. Usually, this occurs when users forgot their passwords, but someone else may be trying to guess passwords, so it deserves to be examined.
- Novell NetWare and Windows servers enable you to establish limits on when and where a user can log in to the network. You can establish times of day that a user is allowed to log in, and you can also restrict a user account to particular network computers. Doing so for all users on the network is usually overkill, but you might want to consider restricting the administrative account to several different workstations so someone at a different workstation (or coming in through a WAN connection) cannot log in to the account, even if that person somehow knows the password.

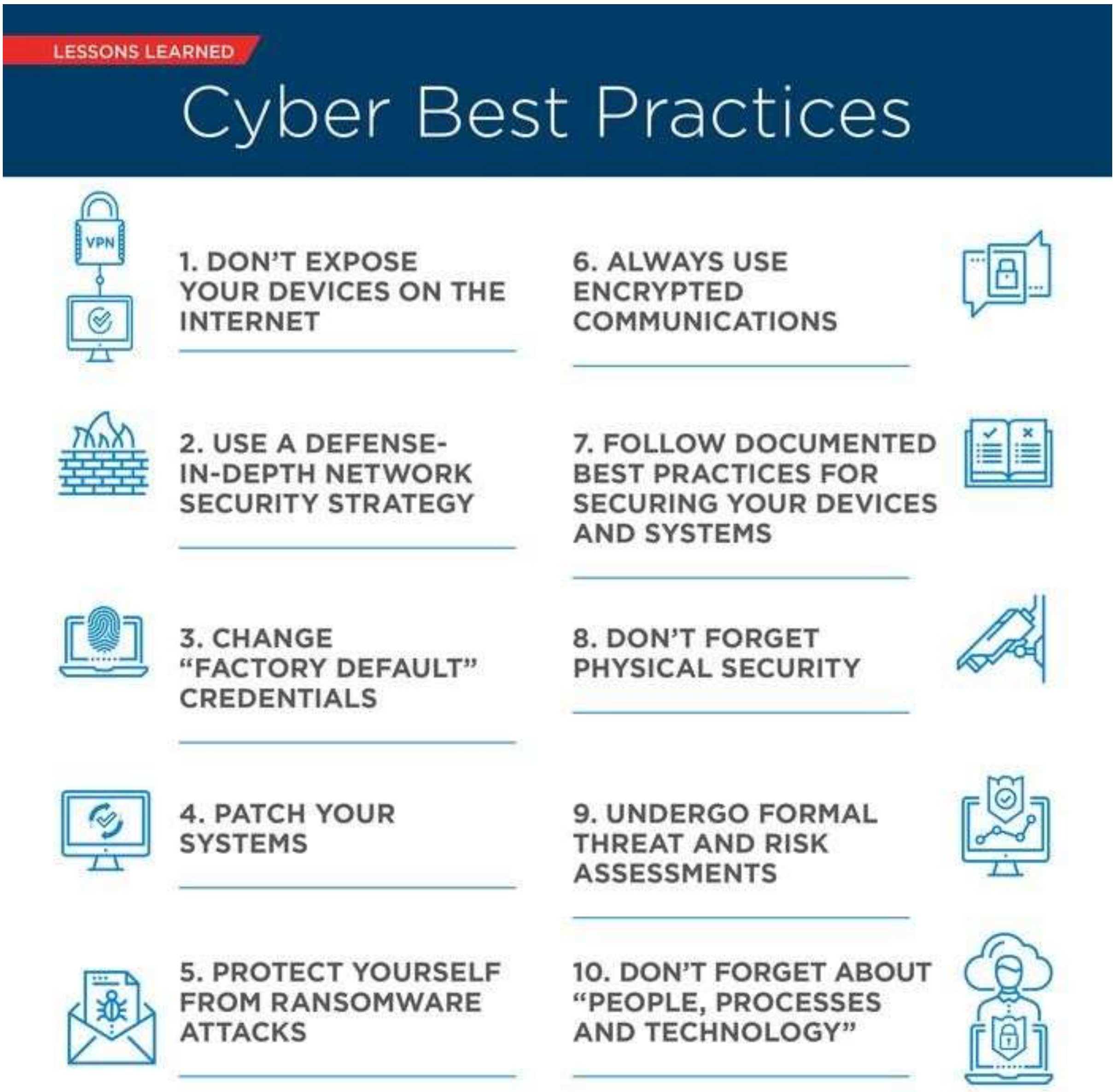
File and Directory Permissions

Another type of internal security that you need to maintain for information on your network involves the users' access to files and directories. These settings are actually a bit tougher to manage than user accounts, because you usually have at least 20 directories and several hundred files for every user on the network. The sheer volume of directories and files makes managing these settings a more difficult job. The solution is to establish regular procedures, follow them, and then periodically spot-audit parts of the directory tree, particularly areas that contain sensitive files. Also, structure the overall network directories so that you can, for the most part, simply assign permissions at the top levels. These permissions will "flow down" to subdirectories automatically, which makes it much easier to review who has access to which directories. Network operating systems allow considerable flexibility in setting permissions on files and directories. Using the builtin permissions, you can enable users for different roles in any given directory. These roles control what the user can and cannot do within that directory. Examples of generic directory roles include the following:

- Create only This type of role enables users to add a new file to a directory, but restricts them from seeing, editing, or deleting existing files, including any they've created. This type of role is suitable for allowing users to add new information to a directory to which they shouldn't otherwise have access. The directory becomes almost like a mailbox on a street corner: You can only put new things in it. Of course, at least one other user will have full access to the directory to retrieve and work with the files.
- Read only This role enables users to see the files in a directory and even to pull up the files for viewing on their computer. However, the users cannot edit or change the stored files in any way. This type of role is suitable for allowing users to view information that they should not change. (Users with read privileges can copy a file from a read-only directory to another directory and then do whatever they like with the copy they made. They simply cannot change the copy stored in the read-only directory itself.)
- Change This role lets users do whatever they like with the files in a directory, except give other users access to the directory.

- Full control usually reserved for the “owner” of a directory, this role enables the owners to do whatever they like with the files in a directory and to grant other users access to the directory.

These roles are created in different ways on different network operating systems. Just as you can set permissions for directories, you can also set security for specific files. File permissions work similarly to directory permissions. For specific files, you can control a user’s ability to read, change, or delete a file. File permissions usually override directory permissions. For example, if users had change access to a directory, but you set their permission to access a particular file in that directory to readonly, they would have only read-only access to that file.



LESSONS LEARNED

Cyber Best Practices

1. DON’T EXPOSE YOUR DEVICES ON THE INTERNET

2. USE A DEFENSE-IN-DEPTH NETWORK SECURITY STRATEGY

3. CHANGE “FACTORY DEFAULT” CREDENTIALS

4. PATCH YOUR SYSTEMS

5. PROTECT YOURSELF FROM RANSOMWARE ATTACKS

6. ALWAYS USE ENCRYPTED COMMUNICATIONS

7. FOLLOW DOCUMENTED BEST PRACTICES FOR SECURING YOUR DEVICES AND SYSTEMS

8. DON’T FORGET PHYSICAL SECURITY

9. UNDERGO FORMAL THREAT AND RISK ASSESSMENTS

10. DON’T FORGET ABOUT “PEOPLE, PROCESSES AND TECHNOLOGY”

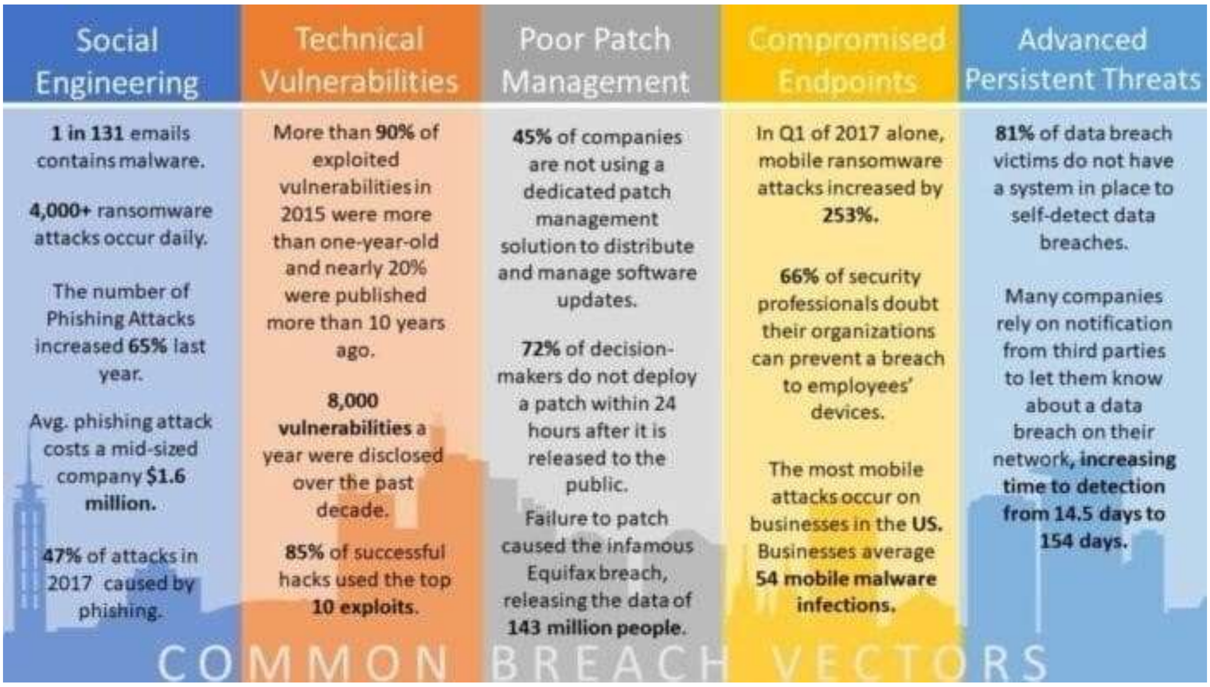
Understanding External Threats

External security is the process of securing the network from external threats. Before the Internet, this process wasn’t difficult. Most networks had only external modems for users to dial in to the network, and it was easy to keep those access points secure. However, now that nearly all networks are connected to the Internet, external security becomes much more important and also much more difficult. At the beginning of this study unit, I said that no network is ever totally secure. This is especially true when dealing with external security for a network connected to the Internet. Almost daily, crackers discover new techniques that they can use to breach the security of a network through an Internet connection. Even if you were to find a book that discussed all the threats to a specific type of network, the book would be out of date soon after it was printed. Three basic types of external security threats exist:

- Front-door threats: These threats arise when a person from outside the company somehow finds, guesses, or cracks a user password and then logs on to the network. The perpetrator could be someone who had an association with the company at some point or could be someone totally unrelated to the company.

- Back-door threats: These are threats where software or hardware bugs in the network's operating system and hardware enable outsiders to crack the network's security. After accomplishing this, the outsiders often find a way to log in to the administrative account and then can do anything they like. Back-door threats can also be deliberately programmed into software you run.

- Denials of service (DoS): DoS attacks deny service to the network. Examples include committing specific actions that are known to crash different types of servers or flooding the company's Internet connection with useless traffic (such as a flood of ping requests).



Social Engineering	Technical Vulnerabilities	Poor Patch Management	Compromised Endpoints	Advanced Persistent Threats
1 in 131 emails contains malware. **4,000+** ransomware attacks occur daily. The number of Phishing Attacks increased **65%** last year. Avg. phishing attack costs a mid-sized company **$1.6 million.** **47%** of attacks in 2017 caused by phishing.	More than **90%** of exploited vulnerabilities in 2015 were more than one-year-old and nearly 20% were published more than 10 years ago. **8,000 vulnerabilities** a year were disclosed over the past decade. **85%** of successful hacks used the top **10 exploits.**	**45%** of companies are not using a dedicated patch management solution to distribute and manage software updates. **72%** of decision-makers do not deploy a patch within 24 hours after it is released to the public. Failure to patch caused the infamous Equifax breach, releasing the data of **143 million people.**	In Q1 of 2017 alone, mobile ransomware attacks increased by **253%.** **66%** of security professionals doubt their organizations can prevent a breach to employees' devices. The most mobile attacks occur on businesses in the **US.** Businesses average **54 mobile malware infections.**	**81%** of data breach victims do not have a system in place to self-detect data breaches. Many companies rely on notification from third parties to let them know about a data breach on their network**, increasing time to detection from 14.5 days to 154 days.**

Viruses and Other Malicious Software

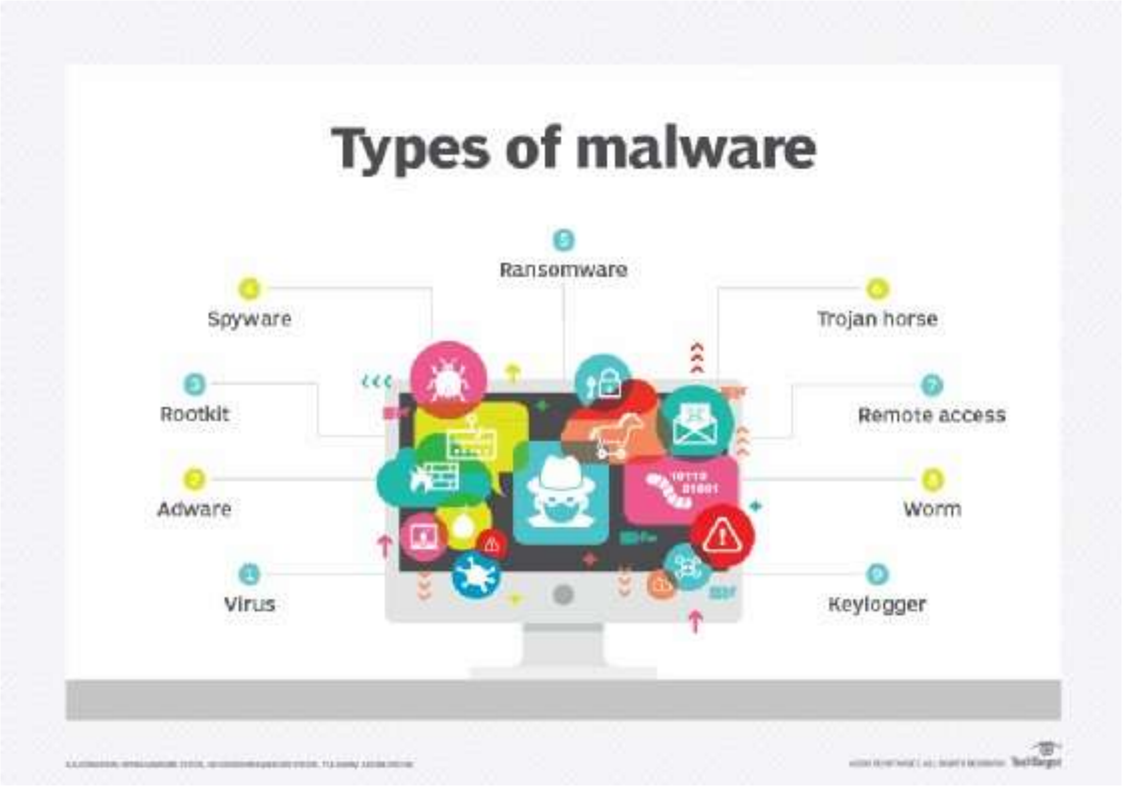
Unfortunately, an increasing array of malicious software is circulating around the world. Many different types of this software exist, including the following:

- Viruses A computer virus is a program that spreads by infecting other files with a copy of itself. Files that can be infected by viruses include program files (COM, EXE, and DLL) and document files for applications that support macro languages sophisticated enough to allow virus behavior. (Microsoft Word and Excel are common targets of macro-based viruses.) Sometimes even data files like JPEG image files can be infected by sophisticated viruses.

- Worms A worm is a program that propagates by sending copies of itself to other computers, which run the worm and then send copies to other computers. Recently, worms have spread through email systems like wildfire. One way they spread is by attaching to e-mail along with a message that entices the recipients to open the attachment. The attachment contains the worm, which then sends out copies of itself to other people defined in the user's e-mail address book, without the user knowing that this is happening. Those recipients then have the same thing happen to them. A worm like this can spread rapidly through the Internet in a matter of hours.

- Trojan horses A Trojan horse is a program that purports to do something interesting or useful and then performs malicious actions in the background while the user is interacting with the main program.

- Logic bombs Logic bombs are malicious pieces of programming code inserted into an otherwise normal program. They are often included by the program's original author or by someone else who participated in developing the source code. Logic bombs can be timed to execute at a certain time, erasing key files or performing other actions.



STUDY UNIT SUMMARY

In this study unit, you learned about common security threats and read advice that can help you formulate and implement good security practices. You should seriously consider retaining an outside security consultant to help you set up your security plans and to review and audit them on a regular basis. Even in an entire book devoted to the subject of network security, you can't learn all you need to know to make a network as secure as possible. New threats are discovered constantly, and the changing software landscape makes such information quickly obsolete. If you're responsible for network security, you should know it's a job that never sleeps, and you can never know enough about it. You need to spend time learning more of the ins and outs of network security, particularly for the operating systems that you use on your network. The following books can help further your network security education.

5.1.10 Revision Questions

Answer the compulsory revision questions below.

a) What do you understand by Malware
b) Which malicious software do you think is the most dangerous
c) Why must you keep your anti-virus constantly updated

https://www.youtube.com/watch?v=6Jubl1UnJTE

https://www.youtube.com/watch?v=IkfggBVUJxY

15. NETWORK SECURITY

Purpose	The purpose of this unit is for the learner to be able to understand how to identify and alleviate any disaster which might occur on a network.
Learning Outcomes	By the end of this unit, you will be able to: • Assessing Disaster Recovery Needs • Describing Critical Components • Network Backup And Restore Procedures • Acquiring Backup Media And Technologies
Time	It will take you 1 Hour to make your way through this unit.
Important terms and definitions	• BACKUP

6.1. INTRODUCTION

Network servers contain vital resources for a company, in the form of information, knowledge, and invested work product of the company's employees. If they were suddenly and permanently deprived of these resources, most companies would not be able to continue their business uninterrupted and would face losing millions of dollars, both in the form of lost data and the effects of that loss. Therefore, establishing a network disaster recovery plan and formulating and implementing the network's backup strategy are the two most important jobs in network management. In this study unit, you learn about the issues that you should address in a disaster recovery plan, and also about network backup strategies and systems. Before getting into these topics, however, you should read about the City of Seattle's disaster recovery experiences.

DISASTER RECOVERY PLANS

A disaster recovery plan is a document that explores how a network recovers from a disaster that either imperils its data or stops its functioning. A company's external financial auditors often require annual disaster recovery plans, because of the data's importance to the business and the effect that such a network failure would have on a company. Moreover, disaster recovery plans are also important because they force the manager of the network to think through all possible disaster scenarios. By taking these scenarios into account, the manager can make more effective plans to protect the network's data from loss and to restore full operations of the business as quickly as possible. As mentioned at the beginning of this study unit, planning for disaster recovery and managing the company's backup systems are a network manager's two most important jobs.

Most companies do not have extremely long disaster recovery plans. For a single network of up to several hundred nodes and 15 or so servers, such a plan usually consists of about 10 to 20 pages or fewer, although its length varies depending on the complexity of the company's network operations. Fortune 500 companies, for instance, may have disaster recovery plans that are several hundred pages long, when all sites are considered in aggregate. One strategy to keep disaster recovery plans concise and to maximize their usefulness is to focus on problems that, while remote, are at least somewhat likely to occur. Alternatively, you can focus on disaster results—what happens—rather than trying to cover disaster causes—why it happened. Focusing your plan on disaster results means contemplating problems such as loss of a single server, loss of the entire server room, loss of all of the customer service workstation computers, and so forth, without worrying about the possible disasters that might cause those results. The following sections discuss the minimum key issues that a disaster recovery plan should address. Depending on your own company, your plan may need to address additional issues

ASSESSING DISASTER RECOVERY NEEDS

Before drafting the actual plan, you should first assess the needs that the plan must meet. These needs will vary depending on who requires input into the disaster recovery planning process and what issues these people want the plan to address. Consider these types of needs:

- Formally planning for contingencies and ensuring that all possible disasters have been considered, and defining countermeasures in the plan
- Assuring the company's external accounting auditors that the company has considered and developed plans to handle disasters
- Informing the company's top management about the risks that exist for the network and its data in different situations, and how much time you expect to need to resolve any problems that occur

▪ Soliciting input from top management of the company as to recovery priorities and acceptable minimum requirements to re-establish services.

CONSIDERING DISASTER SCENARIOS

You should start your planning process by considering different possible disaster scenarios. For example, consider the following disasters:

▪ A fire in your server room—or somewhere else in the building—destroys computers and tapes.

▪ Flooding destroys computers and backup batteries low enough to the server room floor to be affected. Remember that floods may be caused by something within the building itself, such as a bad water leak in a nearby room or a fire that activates the fire sprinklers.

▪ An electrical problem of some kind causes power to fail.

▪ Some problem causes total loss of connectivity to the outside world. For example, a critical wide area network (WAN) or Internet link may go down.

▪ A structural building failure of some kind affects the network or its servers.

▪ Any of the preceding problems affects computers elsewhere in the building that are critical to the company's operations. For example, such an event may happen in the manufacturing areas, in the customer service center, or in the telephone system closet or room. While none of these events is very likely, it is still important to consider them all. The whole point of disaster recovery planning is to prevent or minimize serious losses, and the process is much less useful if you consider only those disasters that you think are the most likely. After considering disasters such as those mentioned, you should next consider serious failures that could also affect the operations of the network. Here are some examples:

▪ The motherboard in your main server fails, and the vendor cannot get a replacement to you for three or more days.

▪ Disks in one of your servers fail in such a way that data is lost. If you are running some kind of redundant array of independent disks (RAID) scheme (discussed in Study unit13), plan for failures that are worse than the RAID system can protect. For example, if you use RAID 1 mirrored drives, plan for both sides of the mirror to fail in the same time frame. If you are using RAID 5, plan for any two drives failing at the same time.

▪ Your tape backup drives fails and cannot be repaired for one to two weeks. While this doesn't cause a loss of data in and of itself, it certainly increases your exposure to such an event. You should plan how you would respond to these and any other possible failures. If the motherboard in your main server fails, you may want to move its drives to a compatible computer temporarily. To address disk failure, you should design a plan under which you can rebuild the disk array and restore data from your backups as rapidly as possible. Regarding your tape backup drive, you will likely want to find out how quickly you can acquire an equivalent drive or whether the maker of the tape drive can provide reconditioned replacement drives quickly in exchange for your failed drive. For all of these failures, you will also want to consider the cost of keeping spare parts, or even entire backup servers, available so that you can restore operations as rapidly as possible. You should consider and investigate all of the following types of possible responses:

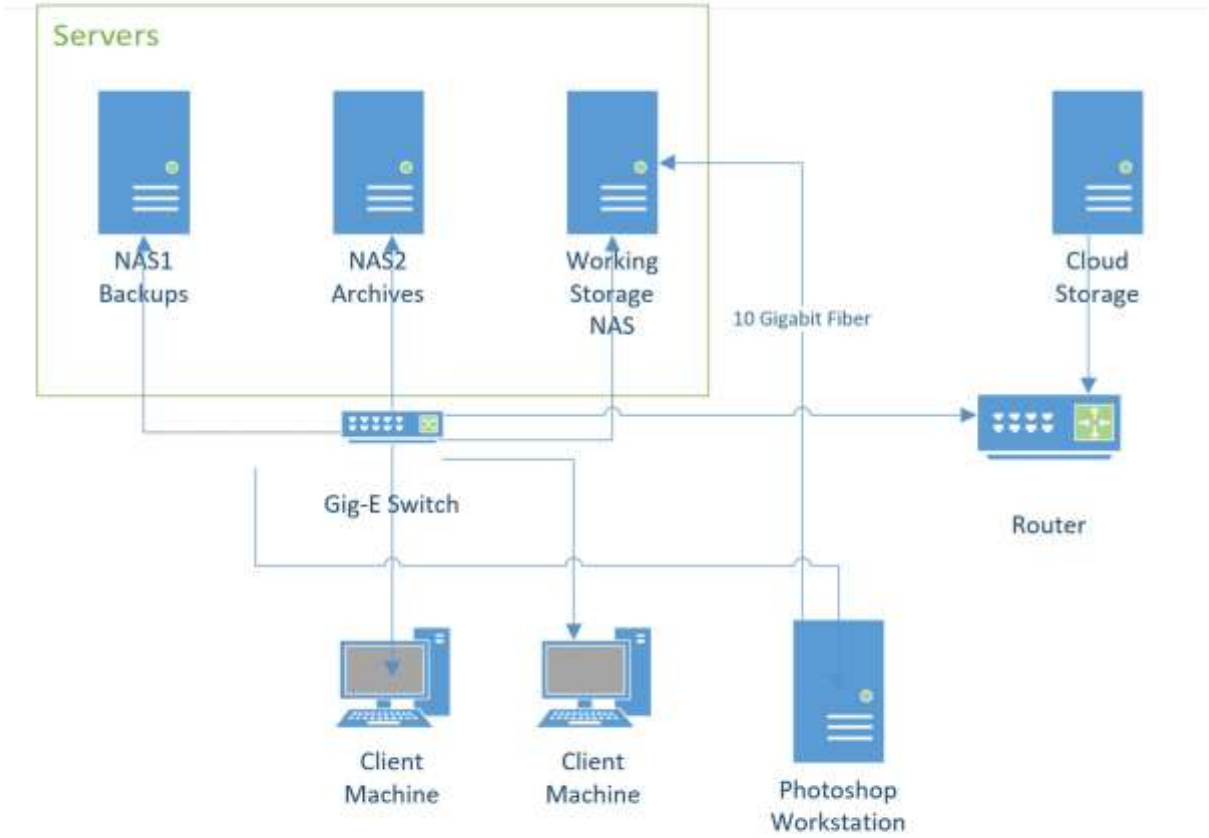
▪ Should you carry a maintenance contract? If so, make sure you thoroughly understand its guarantees and procedures.

▪ Should you stock certain types of parts on hand so that they are readily available in case of failure?
▪ Are other computers available that might work as a short-term replacement for a key server? What about non computer components that are important, such as routers, hubs, and switches?

▪ If you need to take temporary measures, are the affected employees trained to do their jobs with the replacement or with no system at all, if necessary? For example, if a restaurant's electronic systems are down, can the restaurant (and the food servers, kitchen staff, cashiers, and so on) still operate the business manually until the system is repaired?

NETWORK BACKUP AND RESTORE PROCEDURES

A network disaster recovery plan is worthless without some way of recovering the data stored on the server. This is where network backup and restore procedures come in. If you're a network administrator, or aspire to become one, you should already know about the importance of good backups of the system and of important data. If you don't know this, then it's probably the most important lesson that you can take away from this book. Making regular backups is a requirement when using computers—period. You don't need to work with computers for very long before you observe firsthand the importance of good backups. Computers can and do fail and they sometimes fail in ways that render the data stored on them unrecoverable. Also, some turn of events may cause certain important files to be deleted or corrupted. In cases such as these, jobs are saved or lost based on the quality of the backups in place and the ability to restore that important data.



ASSESSING BACKUP NEEDS

Before designing network backup procedures, you must understand the company's backup and restoration needs. Questions such as the following may help in assessing the needs that you must meet:

▪ How dynamic is the data stored on the servers? How often does it change, and in what ways does it change?

▪ How much data needs to be backed up, and at what rate is the amount of data growing?

▪ How much time is available to make the backup? Make sure that you avoid situations where you need to back up terabytes of data using a system that can handle only megabytes per hour.

▪ If a partial or complete restoration from a backup is required, how quickly must it take place? As a rule of thumb, restoring data takes about twice as long as backing it up, although in some cases the times may be approximately equal. In other words, if it takes your backup system 10 hours overnight to back up the entire network, it will take 10 to 20 hours to restore that data—and this estimate doesn't include the time required to resolve whatever problem made it necessary to restore data in the first place.

▪ How coherent does the backed up data need to be? In other words, does a collection of data files need to be handled as a single unit? For example, a directory containing a bunch of word processing files isn't terribly coherent; you can restore one, many, or all of them without much concern about how those restorations will affect other files. On the other hand, a collection of database files for a high-end database is often useless unless you can restore all of the files in the set, from exactly the same point in time. (High-end databases—such as Oracle's—that require this kind of backup will have their own detailed instructions for how backups must be made.)

▪ What is the required trade-off between cost and recoverability? You can design backup systems that operate minute to minute so that if something fails, the systems will not lose any data, and management can place a high degree of confidence in this fact. (A bank, for instance, requires this kind of high-end backup system.) However, such backup systems cost a lot of money and require a lot of administration. Most companies would gladly trade that sort of extreme cost for some lower degree of recoverability, such as nightly backups of the system. What does your company need and what is it willing to pay for?

▪ How many levels of redundancy does the company need in its backups? Most backups are made onto tapes and support servers that use RAID arrays, so the tapes are actually the second level of protection. In some cases, multiple tapes may be required, each with a separate copy of the backup. Or another way to proceed for maximum redundancy is to copy backups to an off-site storage company over some sort of network connection. When making your assessment, it is important to involve the senior management of your company in the process. At a minimum, you should present your findings and seek management's agreement or input.

ACQUIRING BACKUP MEDIA AND TECHNOLOGIES

Once you have some idea of your backup needs, you can then proceed to acquire the necessary hardware and software to create and manage your backups. If you need to purchase new backup hardware for a system, you can choose from a number of proven, good systems, depending on your actual needs. When choosing a backup technology, consider the following factors:

▪ Reliability of the hardware and the media

▪ Cost of the hardware and the media

▪ Storage capacity

▪ Likely frequency of restorations

▪ The importance of fitting the entire backup onto a single piece of media

If your company can afford digital linear tape (DLT) or Linear Tape-Open (LTO) systems and can make use of their capacities, you should definitely look into purchasing this technology. DLT and LTO tapes are rock solid, can be used a rated million times, and are said to have a shelf life of 30 years. Moreover, the drives are fast for both backups and restorations. Finally, robotic auto-changers are available for DLT and LTO drives, which mean that there is plenty of head room if you outgrow the size of your drive. Also, the robotic systems are relatively inexpensive and range from small systems that can hold five tapes up to large libraries that can hold tens or hundreds of tapes. Some newer backup technologies, such as Super DLT S4 (600GB per tape) and LTO-4 (800GB per tape), promise to up DLT's ante. For larger networks, these emerging technologies may make sense. Both DLT and LTO are reliable tape formats with a lot of support from various computer equipment vendors.

CHOOSING BACKUP STRATEGIES

After acquiring all the necessary information, you can plan a backup rotation strategy, which addresses how backup media is rotated. Backup rotations are designed to accomplish the following goals:

▪ Rebuild the system with the most recent data possible, in case of a catastrophic failure

▪ Restore files from older tapes that may have been accidentally erased or damaged without anyone noticing the potential loss of data immediately

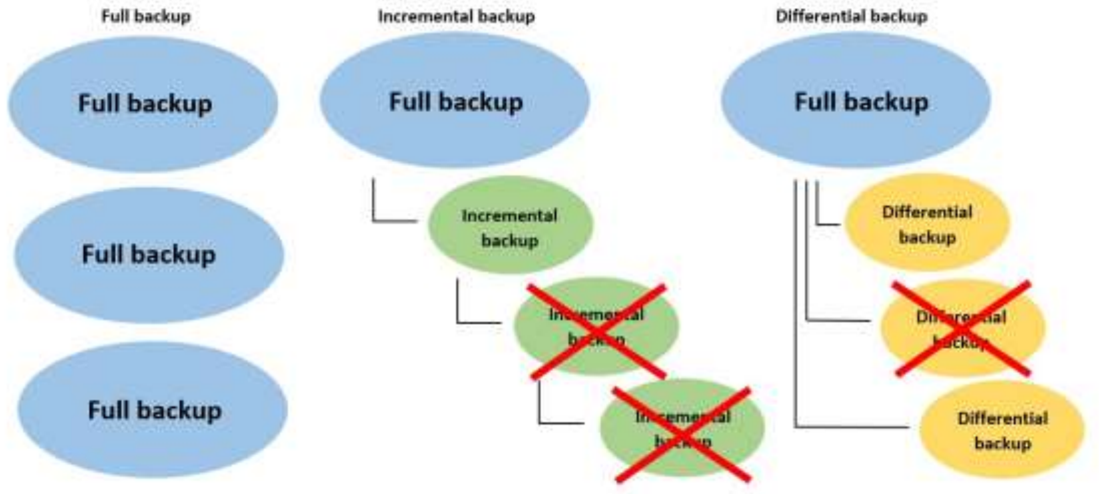
▪ Protect against backup media failure

▪ Protect the data from an environmental failure, such as a fire, that destroys the original system and data. Most network operating systems maintain special bits for each file on the system. One of these is called the archive bit, which indicates the backup status of the file. When a user modifies a file, its archive bit is set to on, indicating that the file should be backed up. When the backup is accomplished, the archive bit is cleared. Using this archive bit and your backup software, you can make the following types of backups:

▪ A full backup, where all selected directories and files are backed up, regardless of their archive bit state. Full backups clear the archive bit on all of the backed-up files when they are finished.

▪ An incremental backup, where only files with their archive bit set are backed up. This backs up all files changed since the last full or incremental backup. Incremental backups clear the archive bit of the backed-up files; those files will not be backed up during the next incremental 119 backup unless they are modified again and their archive bits are reset to the on-state. Incremental backups generally minimize the amount of time needed to perform each daily backup, but they take longer to restore and pose a greater risk of media failure.

▪ A differential backup, which is similar to the incremental backup in that it backs up only files with their archive bits set. The key difference in a differential backup is that the archive bits are left turned on. Subsequent differential backups will back up those same files again, plus any new ones that have been modified. Differential backups take longer to make, but reduce the time required to restore and reduce the risk of media failure. In a perfect world, it would be nice always to perform full backups. If the system were to fail, then you would need only the most recent backup tape to restore the system fully. However, for a number of reasons, performing a full backup may not always be feasible. For one thing, perhaps there is inadequate time to perform a full back up each day. Another reason is to extend the life of your media and tape drive by reducing the amount of work that they do. You need to weigh these concerns against the increased time it takes to restore from a combination of full and incremental or differential backups, and the increased possibility of being unable to restore backups properly using a combination approach. (For example, if a full restoration required a full back up from the previous week, plus four incremental backups since then, you're counting on having all five tapes be perfectly good, and you're somewhat more exposed to a bad tape.)One common way to mix these types of backups is to perform a full backup of the system once a week and perform only incremental or differential backups each day of the week.



CLOUD STORAGE

Cloud storage enables applications to upload data to a network of remote, connected servers. Applications can then maintain that data and access it from anywhere. Applications access data using a web-based API that works with client applications.
Storage is available in four main types:

- Personal storage: Services that enable individuals to store data and sync it across multiple devices.
- Public storage: A cloud storage provider that fully manages data for an enterprise offsite.
- Private storage: The cloud storage provider works on premises at an organization's data center.

- Hybrid storage: A mix of public and private cloud storage.

WHY CLOUD STORAGE

Accessibility
Users can access data stored on the cloud from anywhere with internet access, from many different types of devices.

Data recovery
By moving data offsite, companies can help ensure business continuity.

Cost
Enterprises can avoid the expense of buying their own storage equipment by using remote storage owned by cloud providers.

CONSIDERATIONS FOR CLOUD STORAGE

- **Security**
  Because data is accessed online, controls should authenticate applications and users. Companies may also require data encryption.
- **Storage space**
  Cloud storage can become expensive with a large volume of data. Hybrid or on-premises solutions may help manage costs.
- **Bandwidth**
  By using a service that offers multiple locations, load balancing manages network issues. Some storage may benefit from caching.
- **Management interface**
  Providers offer different web-based control panels with their services. Enterprises should choose one with the options they need.

STUDY UNIT SUMMARY

You can be the most proficient person at networking in the world, but if you don't create and carefully manage an appropriate disaster recovery program for your company, you're not doing your job. The importance of this area cannot be overstated. In addition to this study unit, you should also study material covering specific backup and restore instructions for your network operating systems and databases, as well as the documentation for your backup hardware device and the backup software you select. The next study unit discusses key information that you should know about selecting, installing, and managing servers. Servers are the heart of any network, and selecting reliable, productive servers not only will eliminate potential trouble spots for your network, but can also help you avoid needing to actually use the disaster recovery plans and strategies that you have put in place.

5.1.11 Revision Questions

Answer the compulsory revision questions below.

a) Which storage implementation is the latest available today?
b) What is the maximum number of drives that can be used for RAID5?
c) Differentiate between incremental backup and differential backup
d) Which storage devices do you recommend for backup and why?
e) Which backup strategy is used by your organization?

https://www.youtube.com/watch?v=o-83E6levzM

https://www.youtube.com/watch?v=68hbHE6Zk4g

16. REFERENCES

- Network Security: A Beginner’s Guide, Second Edition, by Eric Maiwald (McGrawHill/Professional, 2003)
- Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition, by Stuart McClure, Joel Scambray, and George Kurtz (McGraw-Hill/Professional, 2009)
- Windows 2000 Security Handbook, by Tom Sheldon and Phil Cox (McGraw-Hill/ Professional, 2001)
- https://www.rasmussen.edu/degrees/technology/blog/what-does-a-networkadministrator-do/
- https://www.vonage.com/resources/articles/what-is-wan/
- https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm#:~:text=Advertisements,different%20in%20a%20same%20network
- https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtualdc/active-directory-domain-services-overview
- https://en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line
- https://www.cisco.com/c/en/us/solutions/small-business/resourcecenter/networking/what-is-a-router.html#~types-of-routers https://www.computernetworkingnotes.com/networking-tutorials/network-cabletypes-and-specifications.html

17. VERSION CONTROL

Initials	Version	Date	Description of Amendments
AGC	1.1.2019	19/06/2019	Creation of template
GM	1.2.2019	05/01/2021	Content development